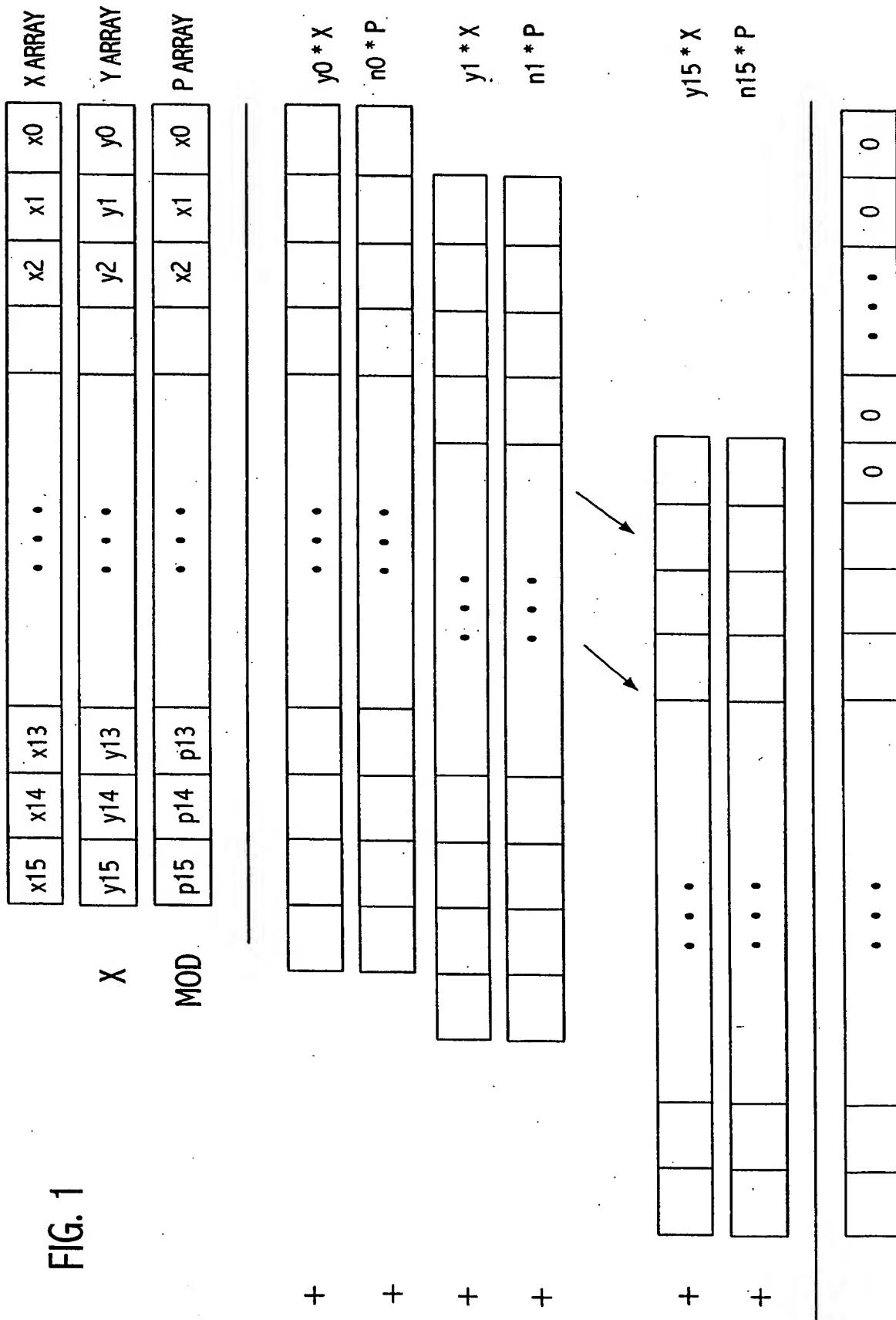


FIG. 1



METHOD AND APPARATUS FOR IMPLEMENTING PROCESSOR
INSTRUCTIONS FOR ACCELERATING PUBLIC-KEY CRYPTOGRAPHY
Inventor(s): Sheueling Chang Shantz et al.

Atty. Dkt. No. 004-30132

2/36

$$\begin{array}{r} \begin{array}{|c|c|c|c|c|c|c|c|c|c|c|c|c|} \hline & x_{15} & x_{14} & x_{13} & & \cdots & & & & x_2 & x_1 & x_0 \\ \hline + & y_{15} & y_{14} & y_{13} & & \cdots & & & & x_2 & x_1 & x_0 \\ \hline \end{array} \\ \hline \begin{array}{|c|c|c|c|c|c|c|c|c|c|c|c|} \hline & s_{16} & s_{15} & s_{14} & s_{13} & & \cdots & & & s_2 & s_1 & s_0 \\ \hline \end{array} \end{array}$$

FIG. 2

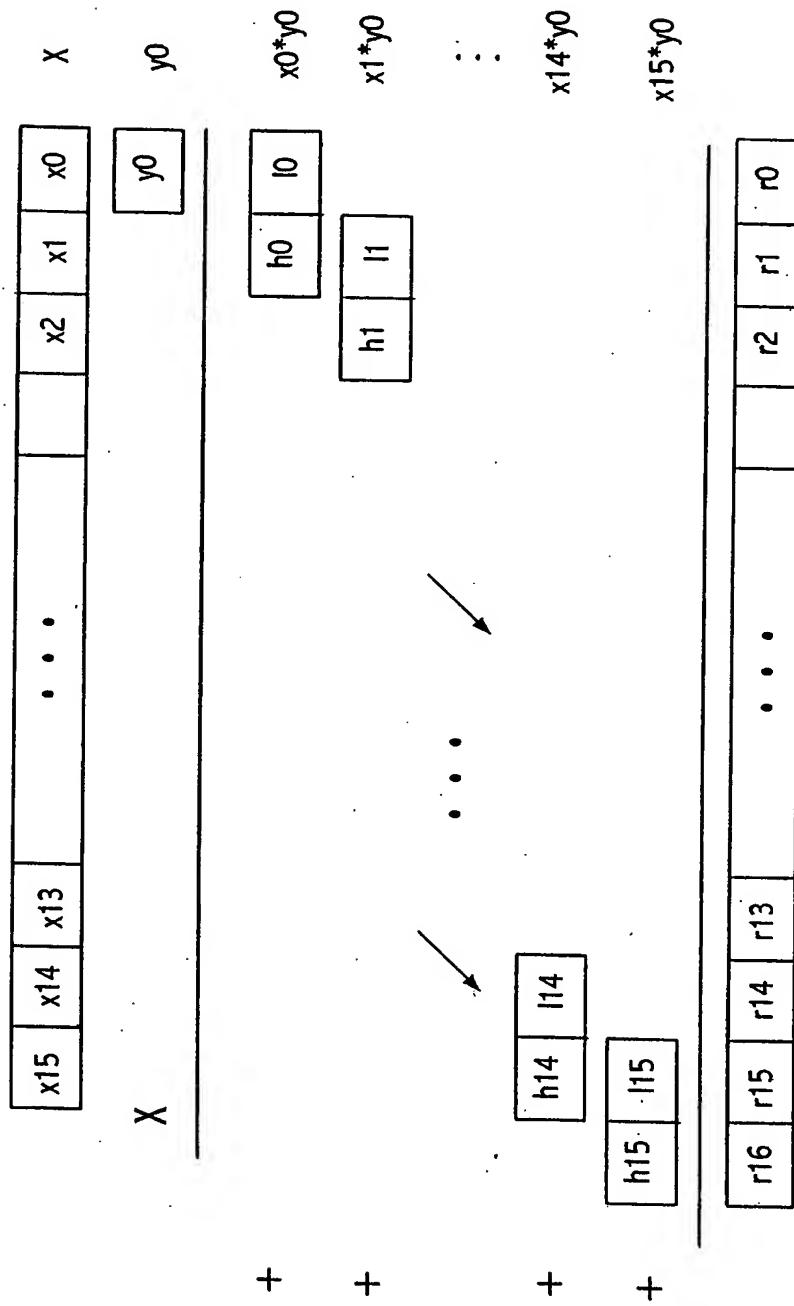


FIG. 3

METHOD AND APPARATUS FOR IMPLEMENTING PROCESSOR
INSTRUCTIONS FOR ACCELERATING PUBLIC-KEY CRYPTOGRAPHY
Inventor(s): Sheueling Chang Shantz et al.

Atty. Dkt. No. 004-30132

4/36

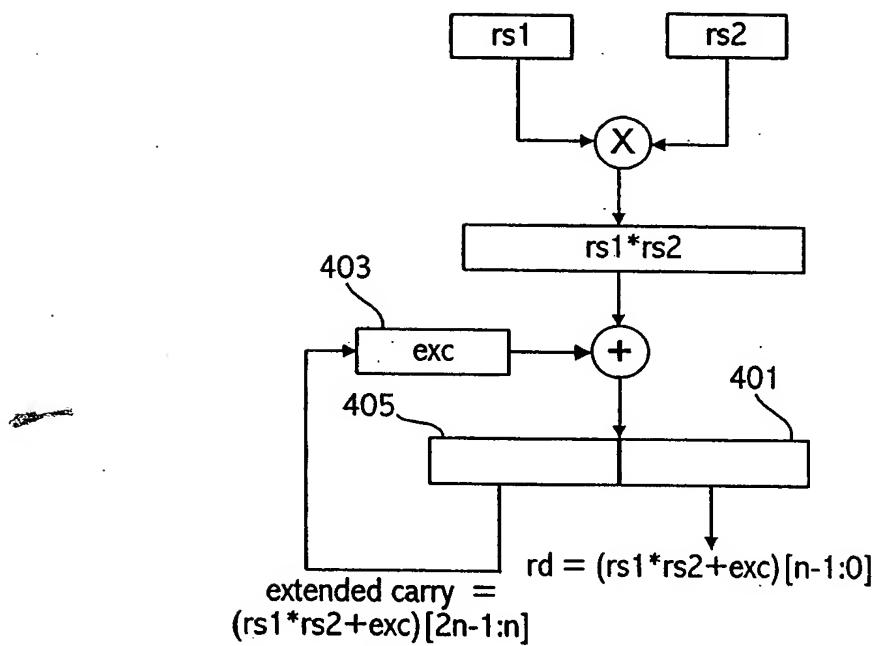


FIG. 4A

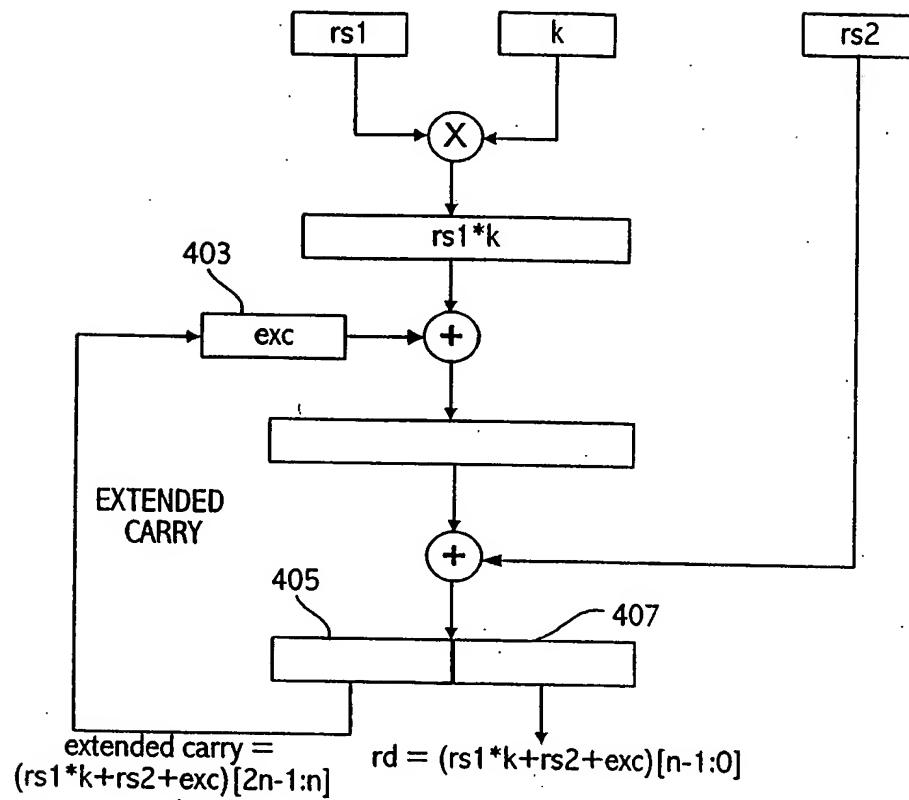


FIG. 4B

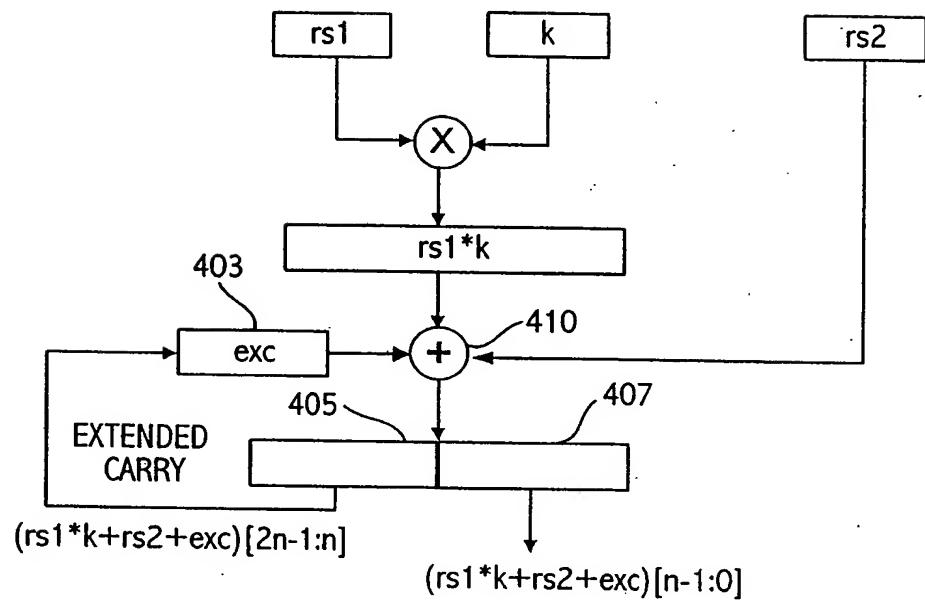


FIG. 4C

METHOD AND APPARATUS FOR IMPLEMENTING PROCESSOR
 INSTRUCTIONS FOR ACCELERATING PUBLIC-KEY CRYPTOGRAPHY
 Inventor(s): Sheueling Chang Shantz et al.

Atty. Dkt. No. 004-30132

7/36

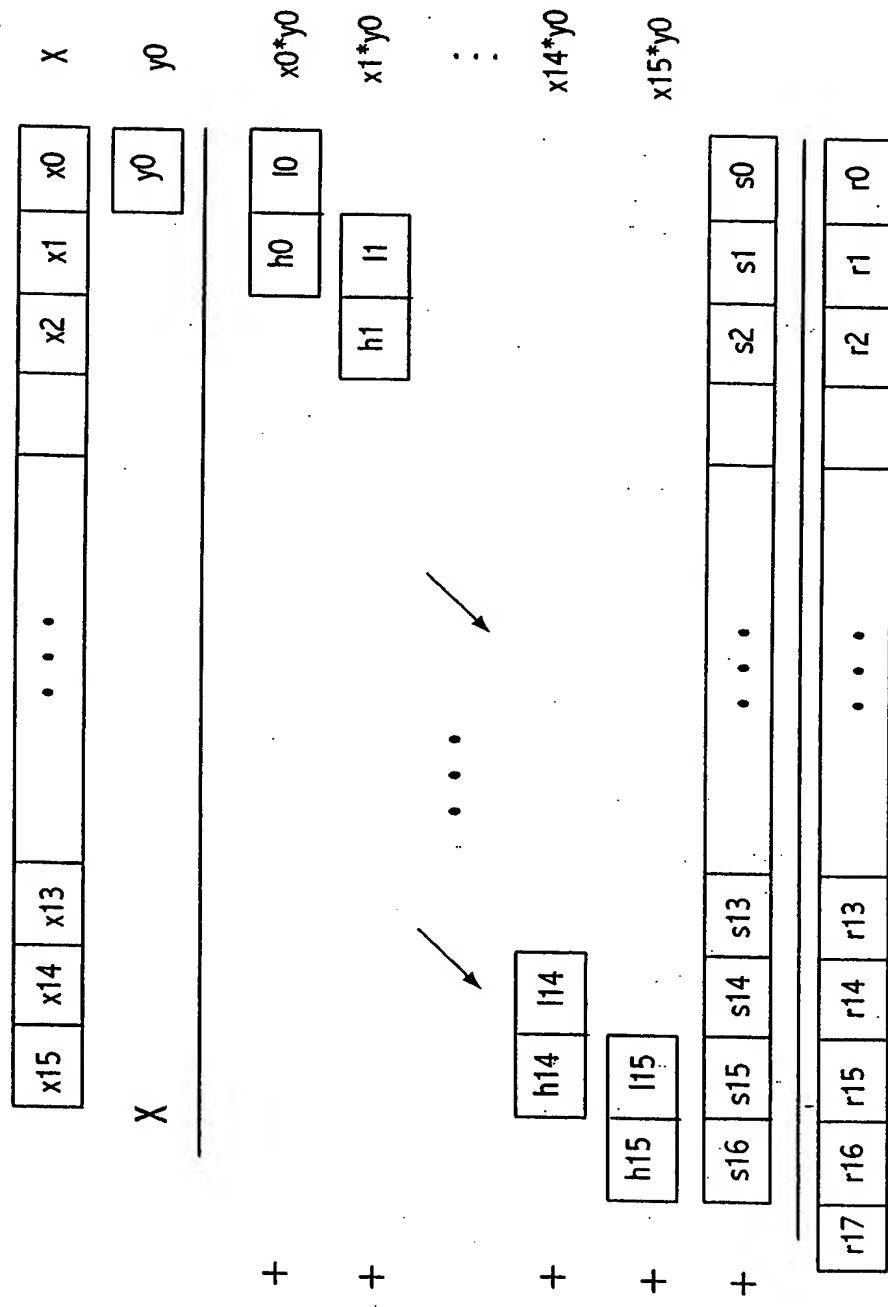


FIG. 5

**METHOD AND APPARATUS FOR IMPLEMENTING PROCESSOR
INSTRUCTIONS FOR ACCELERATING PUBLIC-KEY CRYPTOGRAPHY**
Inventor(s): Sheueling Chang Shantz et al.

Atty. Dkt. No. 004-30132

8/36

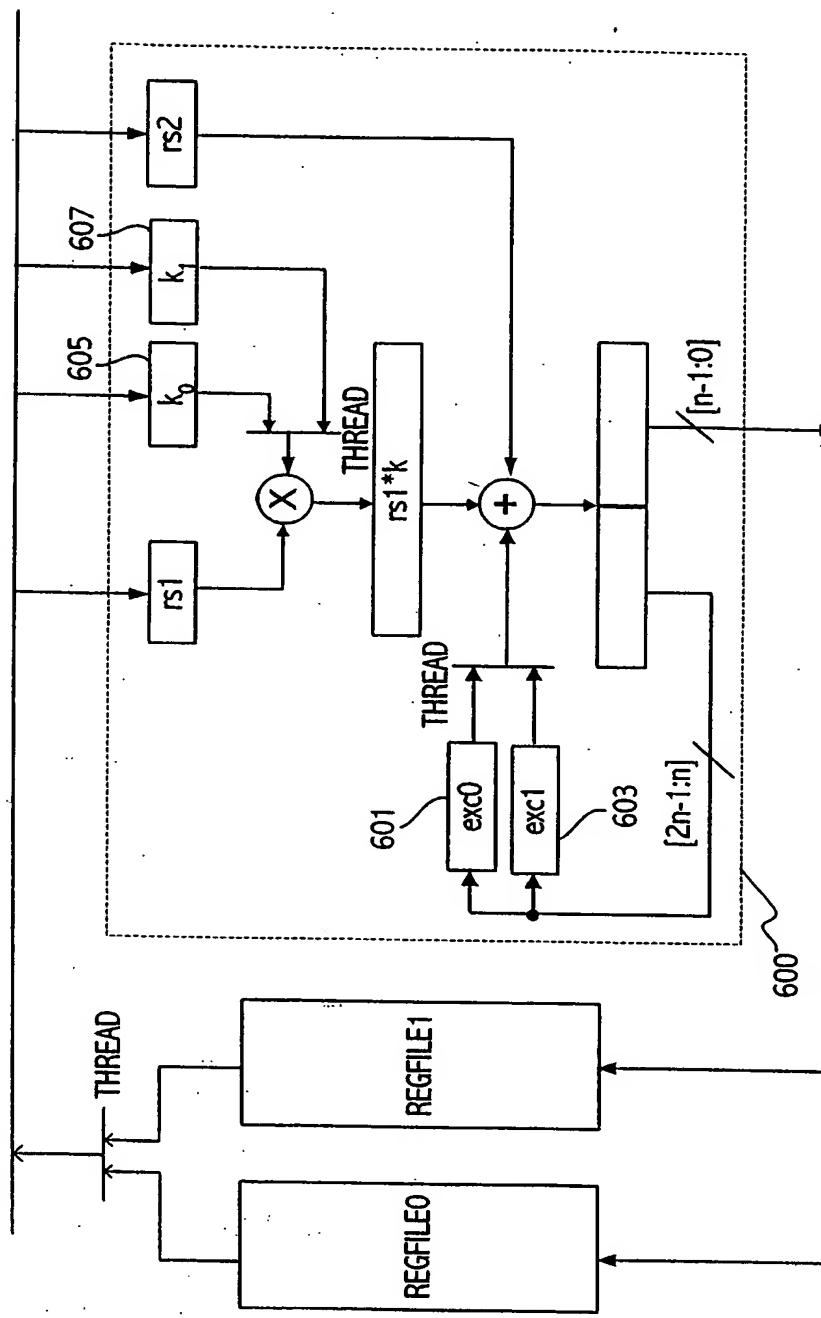


FIG. 6

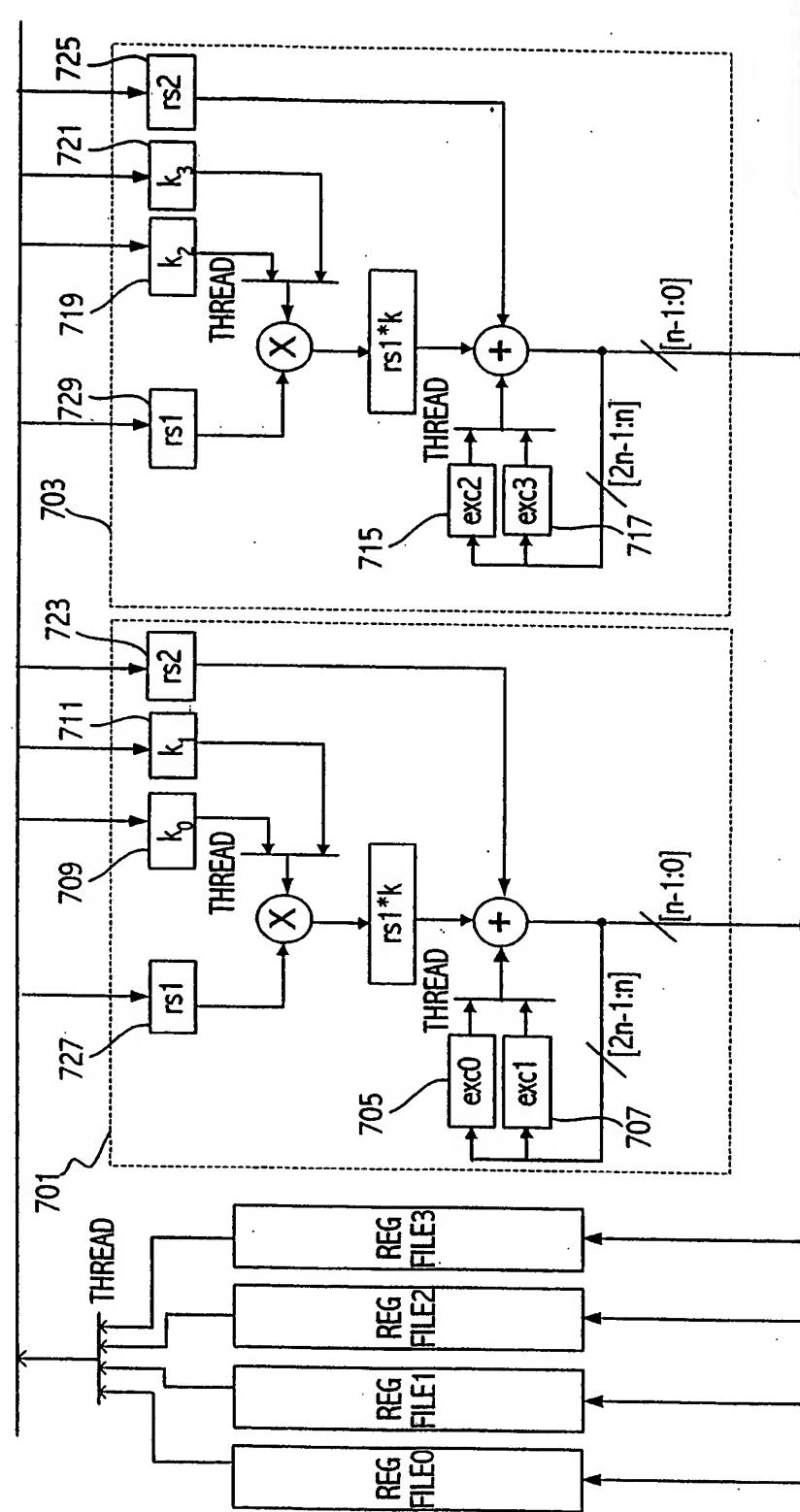


FIG 7

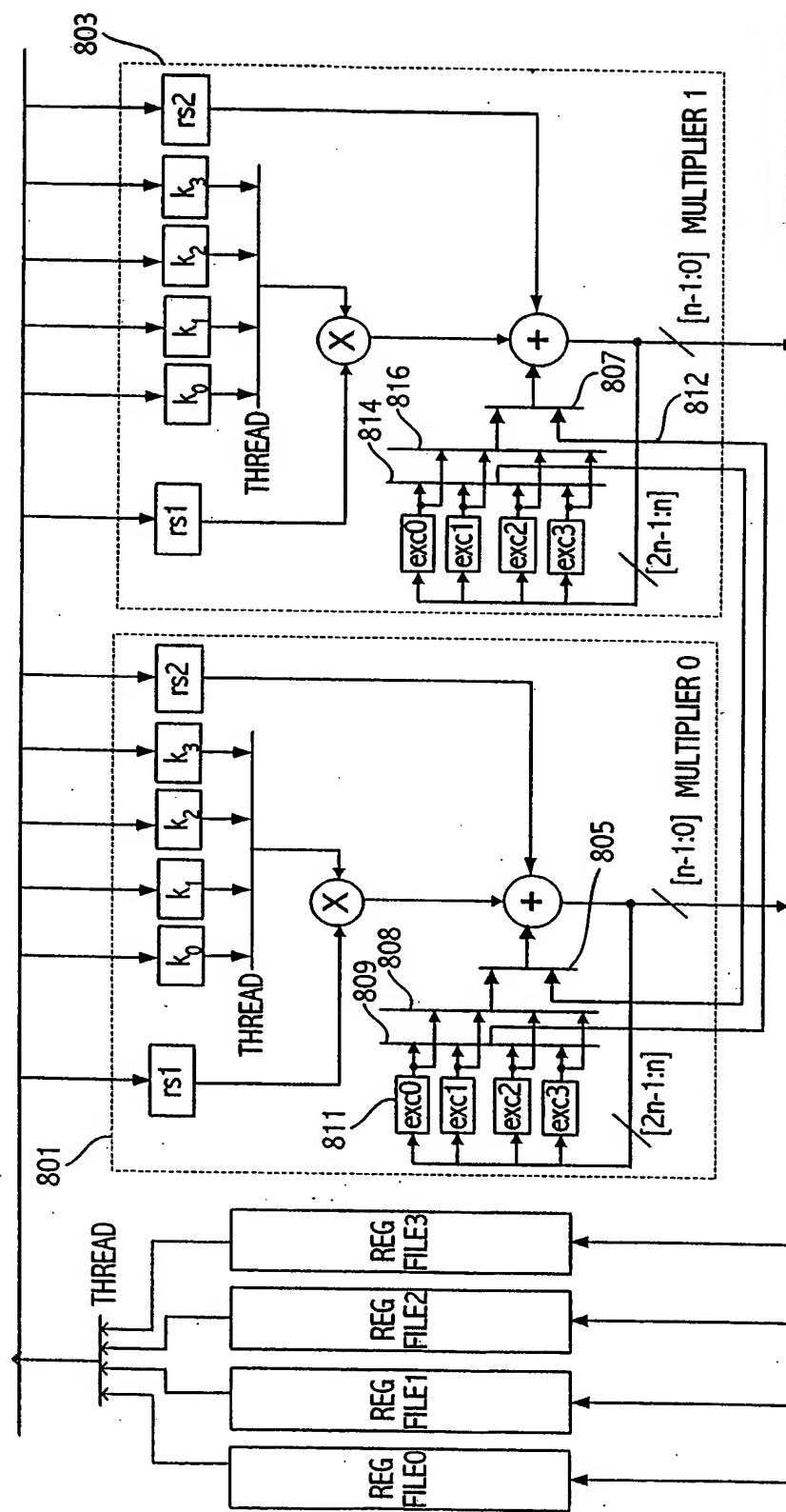


FIG. 8

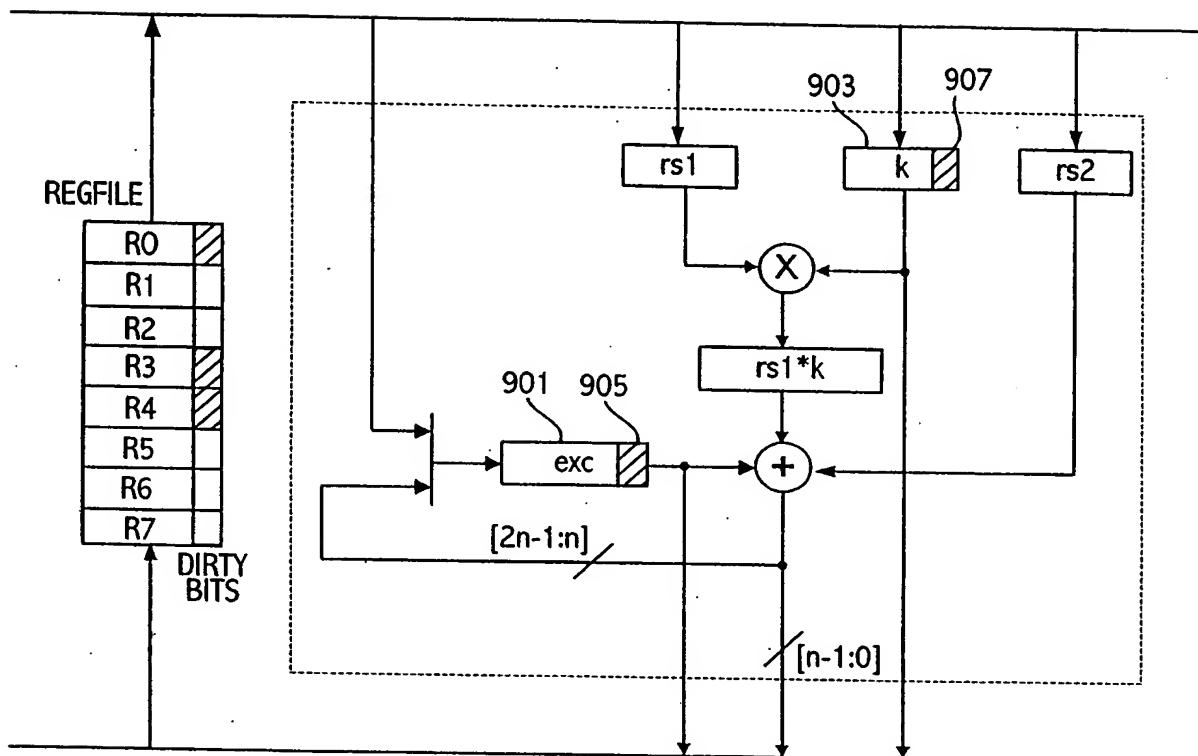


FIG. 9

$$\begin{array}{r}
 X_3 \ X_2 \ X_1 \ X_0 * Y_3 \ Y_2 \ Y_1 \ Y_0 + EX_3 EX_2 EX_1 EX_0 \\
 P_{03} P_{02} P_{01} P_{00} \quad P_{ij} \\
 + \quad P_{13} P_{12} P_{11} P_{10} \\
 + \quad P_{23} P_{22} P_{21} P_{20} \\
 + \quad P_{33} P_{32} P_{31} P_{30} \\
 + \quad EX_3 EX_2 EX_1 EX_0 \\
 \hline
 = \quad S_6 \ S_5 \ S_4 \ S_3 \ S_2 \ S_1 \ S_0 \\
 + C_7 \ C_6 \ C_5 \ C_4 \ C_3 \ C_2 \ C_1 \\
 \hline
 EX_3 EX_2 EX_1 EX_0 \ rd_3 \ rd_2 \ rd_1 \ rd_0
 \end{array}$$

FIG. 10

$$\begin{array}{r}
 X_3 \ X_2 \ X_1 \ X_0 * Y_3 \ Y_2 \ Y_1 \ Y_0 + (0, S_6, S_5, S_4) + (C_7, C_6, C_5, C_4) + (0, 0, 0, CC_4) \\
 P_{03} P_{02} P_{01} P_{00} \\
 + \quad P_{13} P_{12} P_{11} P_{10} \\
 + \quad P_{23} P_{22} P_{21} P_{20} \\
 + \quad P_{33} P_{32} P_{31} P_{30} \\
 + \quad S_6 \ S_5 \ S_4 \leftarrow \text{PREVIOUS SUM OUTPUT} \\
 + \quad C_7 \ C_6 \ C_5 \ C_4 \leftarrow \text{PREVIOUS CARRY OUTPUT} \\
 = \quad S_6 \ S_5 \ S_4 \ S_3 \ S_2 \ S_1 \ S_0 \quad \} \text{NEW WALLACE TREE SUM OUTPUT} \\
 + C_7 \ C_6 \ C_5 \ C_4 \ C_3 \ C_2 \ C_1 \quad \} \text{NEW WALLACE TREE CARRY OUTPUT}
 \end{array}$$

INPUTS AT START OF WALLACE TREE $P_{ij} = X_i * Y_j$

INPUTS IN MIDDLE OF WALLACE TREE

FIG. 11

$$\begin{array}{r}
 S_3 \ S_2 \ S_1 \ S_0 \\
 + \quad C_3 \ C_2 \ C_1 \\
 + \quad CC_4 \\
 \hline
 CC_4 \ RD_3 \ RD_2 \ RD_1 \ RD_0
 \end{array}$$

← PREVIOUS CLA CARRY OUT

← NEW CLA OUTPUT

FIG. 12

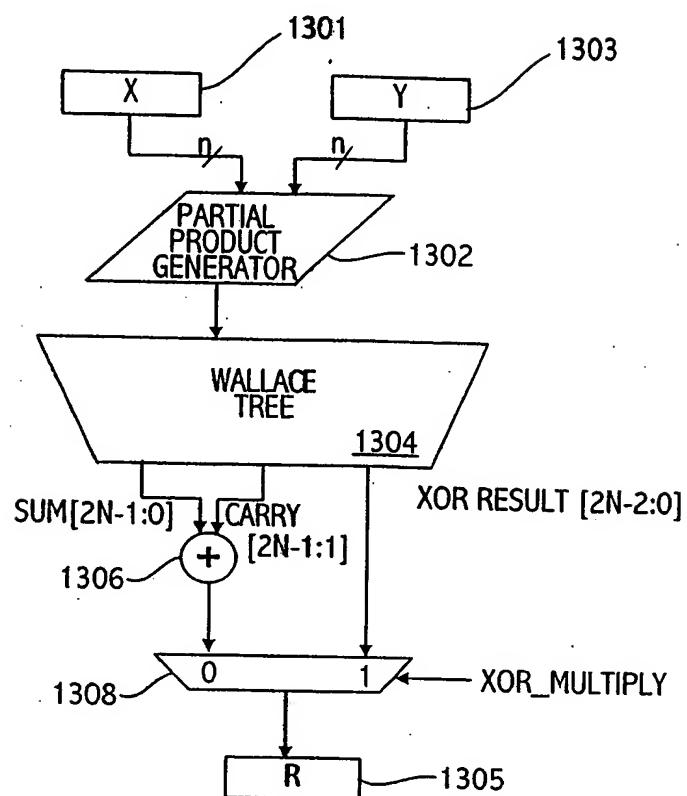


FIG. 13

		-SD	SD	SD	D8	D7	D6	D5	D4	D3	D2	D1	D0
	1	-SE	E8	E7	E6	E6	E4	E3	E2	E1	E0		SD
1	1 -SF	F8 G8	F7 G7	F6 G6	F5 G5	F4 G4	F3 G3	F2 G2	F1 G1	F0 G0	SF		
	H7	H6 H5	H4 H3	H2 H1	H0 SG								
C16	C16	C16 C16	C16 C16	C16 C16	C16 C16	C16 C16	S15 C15	S14 C14	S13 C13	S12 C12	S11 C11	S10 C10	S9 C9
							Z7	Z6	Z5	Z4	Z3	Z2	Z1
C16	C15	C14 C13	C13 C12	C12 C11	C10 C10	C9 C9	C8 C7	C7 C6	C6 C5	C4 C4	C3 C3	C2 C2	C1 C1

with [S7:S0] and [C7:C0] going to the carry look-ahead adder.

Fig 12 B

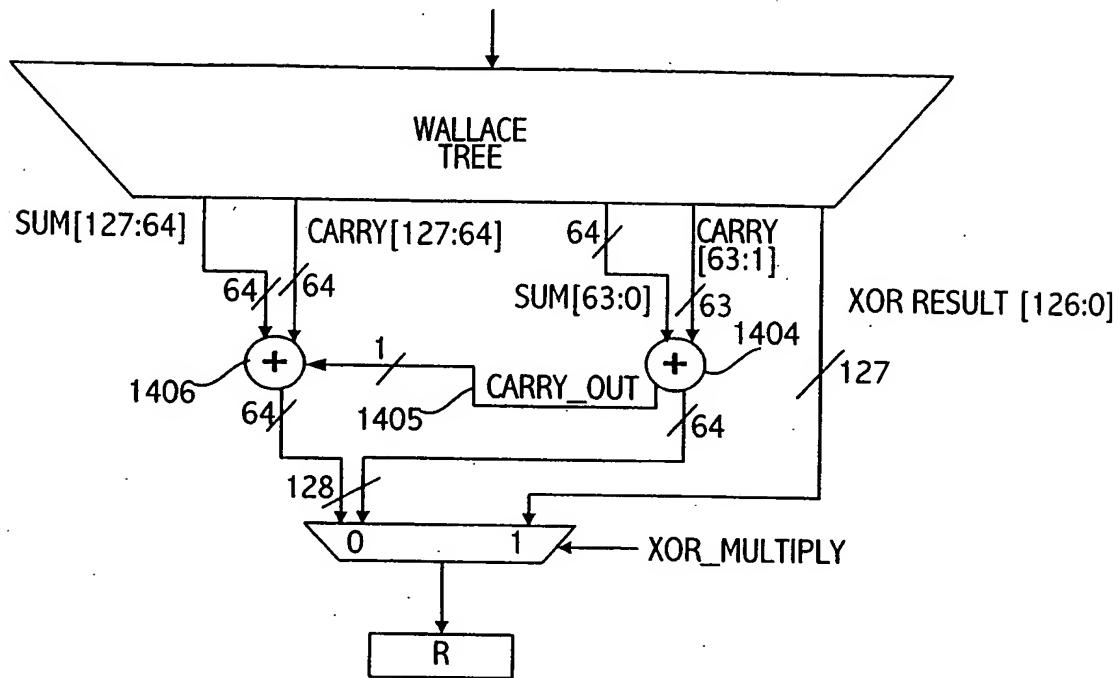


FIG. 14

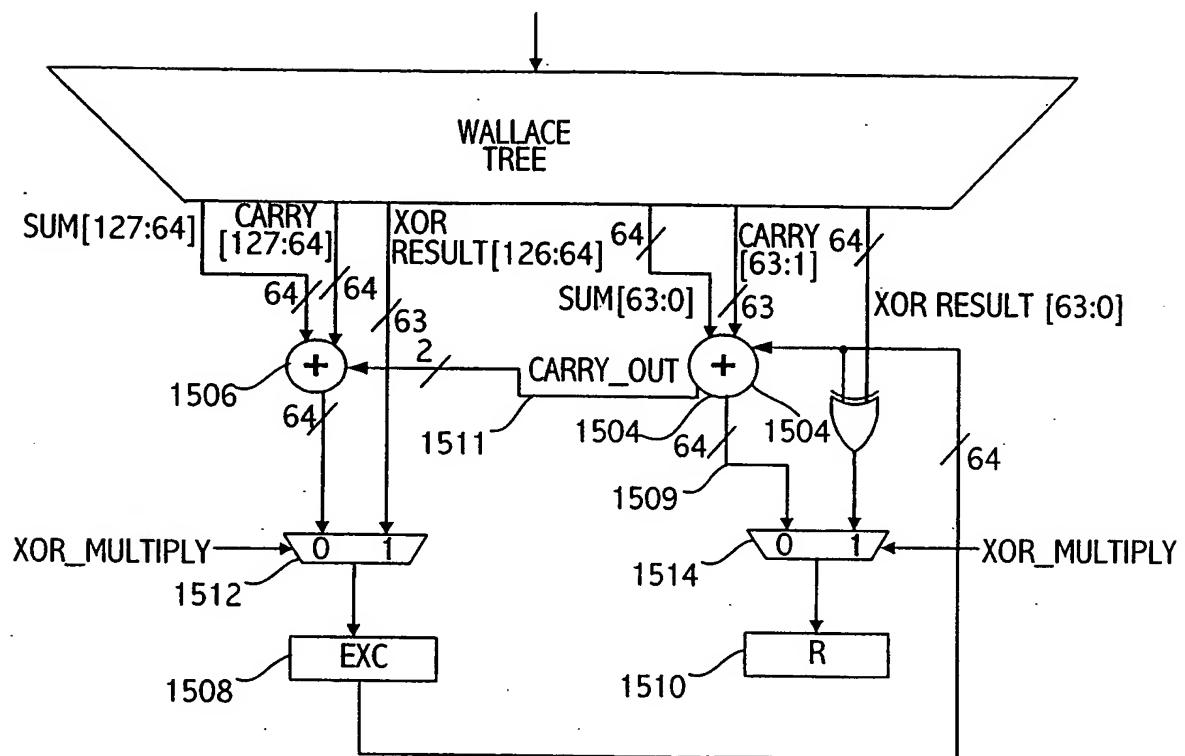


FIG. 15

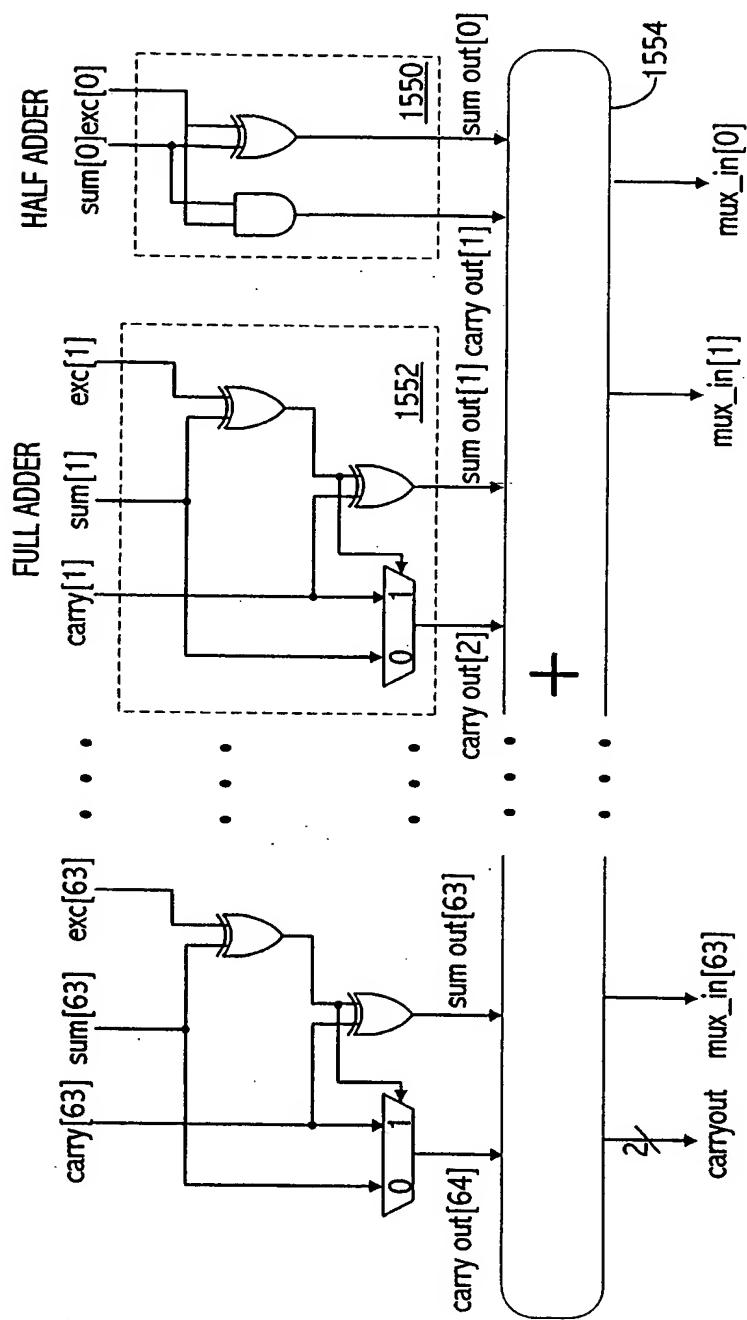


FIG. 15a

METHOD AND APPARATUS FOR IMPLEMENTING PROCESSOR
INSTRUCTIONS FOR ACCELERATING PUBLIC-KEY CRYPTOGRAPHY
Inventor(s): Sheueling Chang Shantz et al.

Atty. Dkt. No. 004-30132

17/36

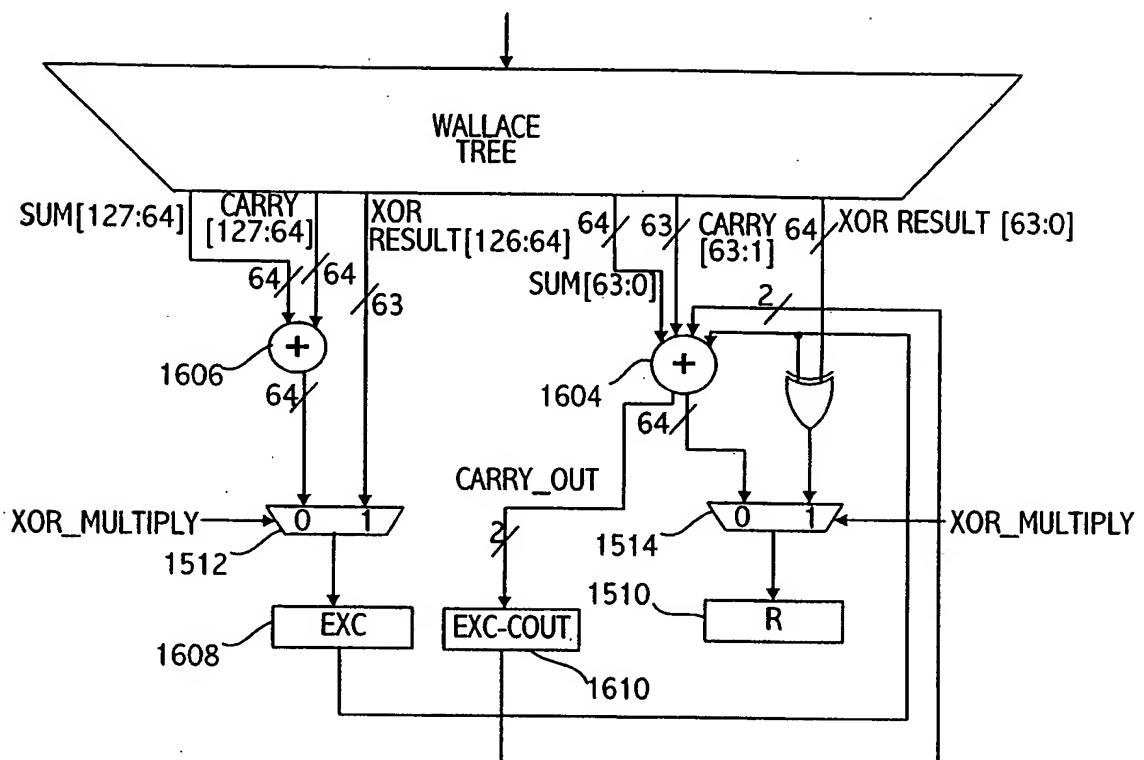


FIG. 16

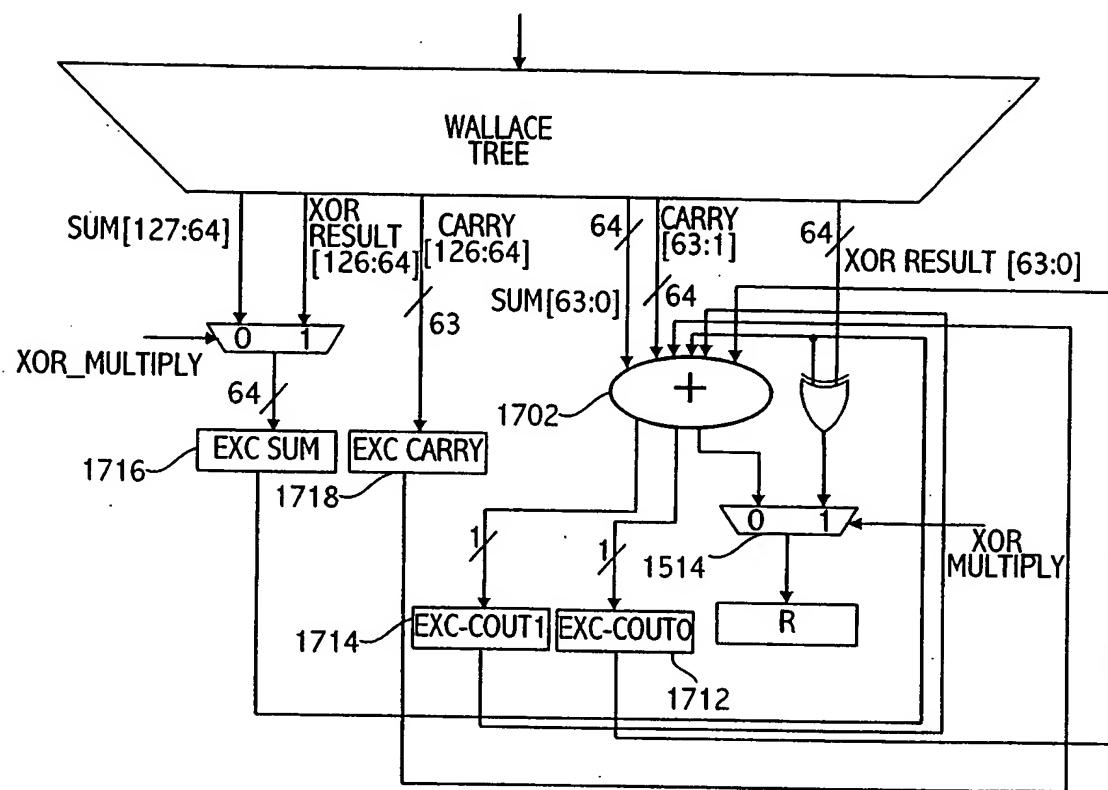


FIG. 17

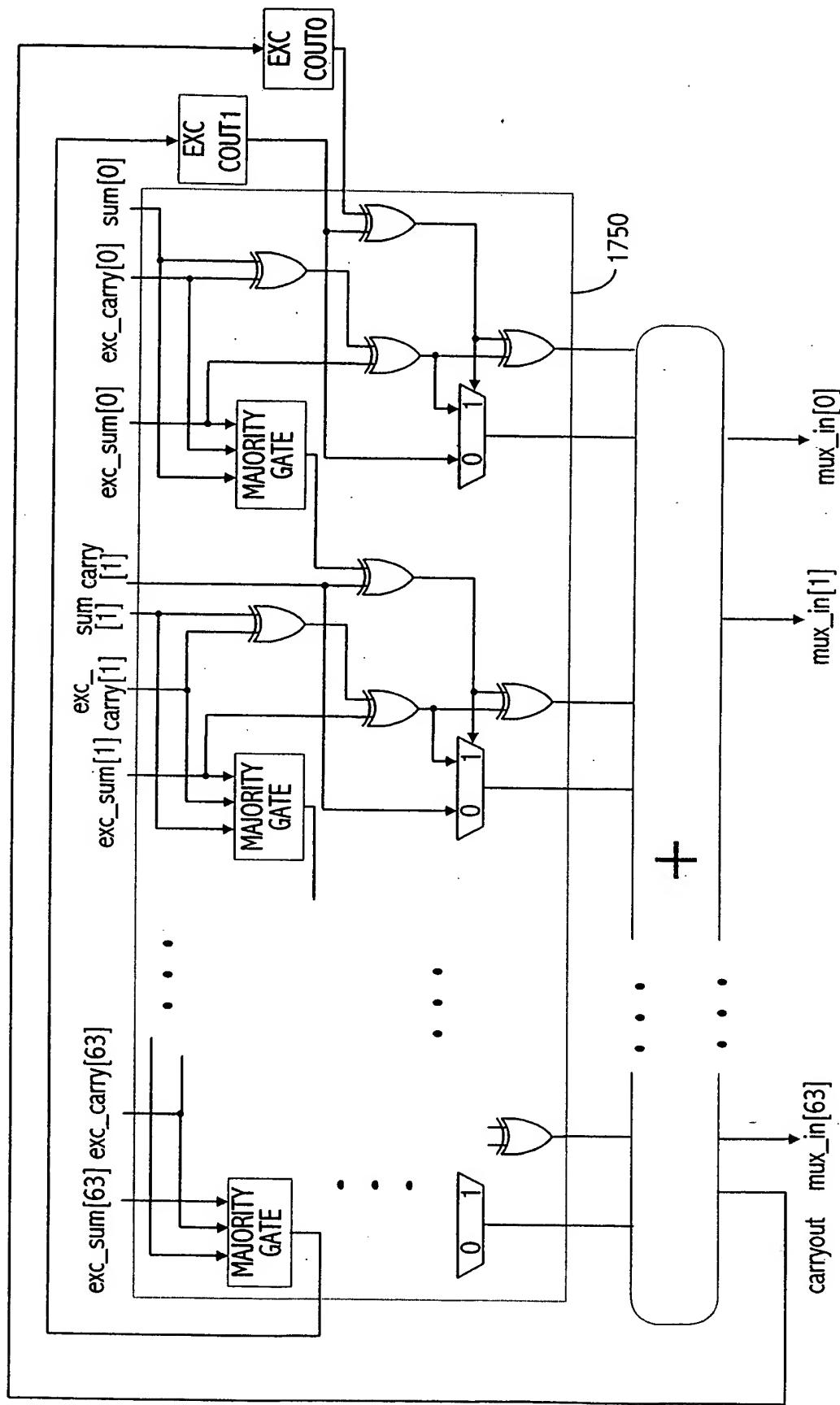


Fig. 17A

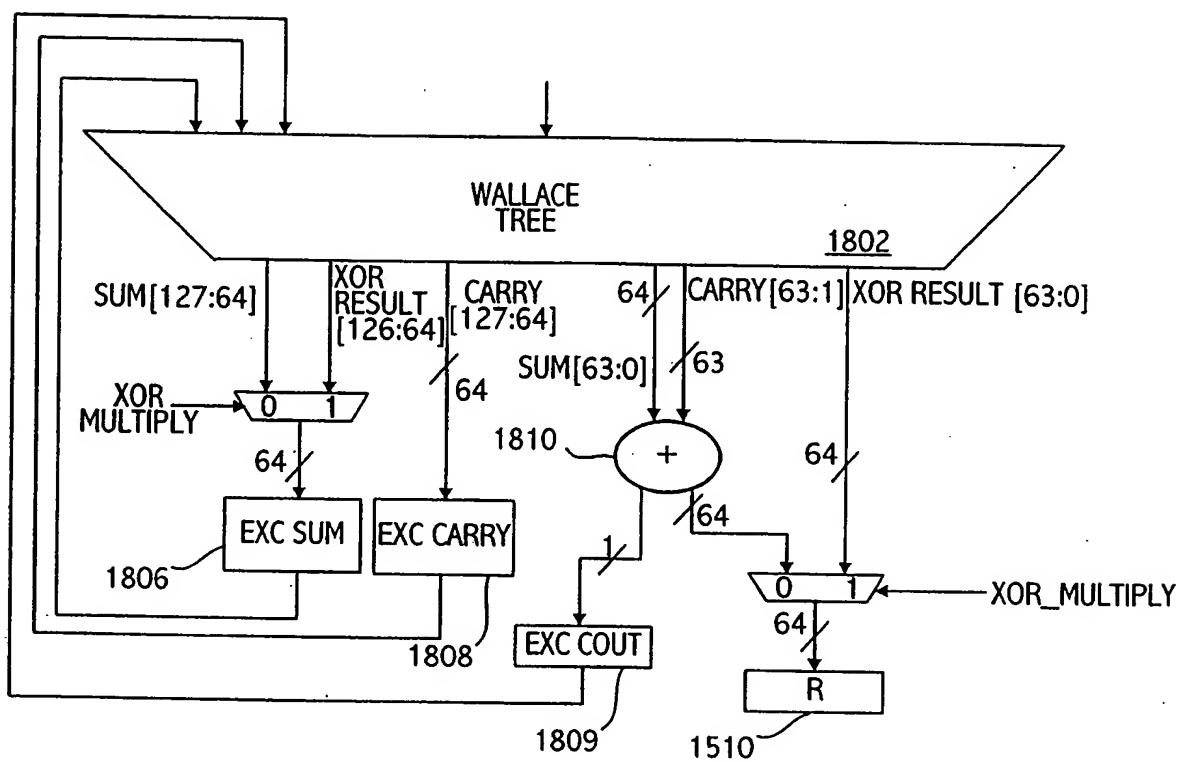


FIG. 18

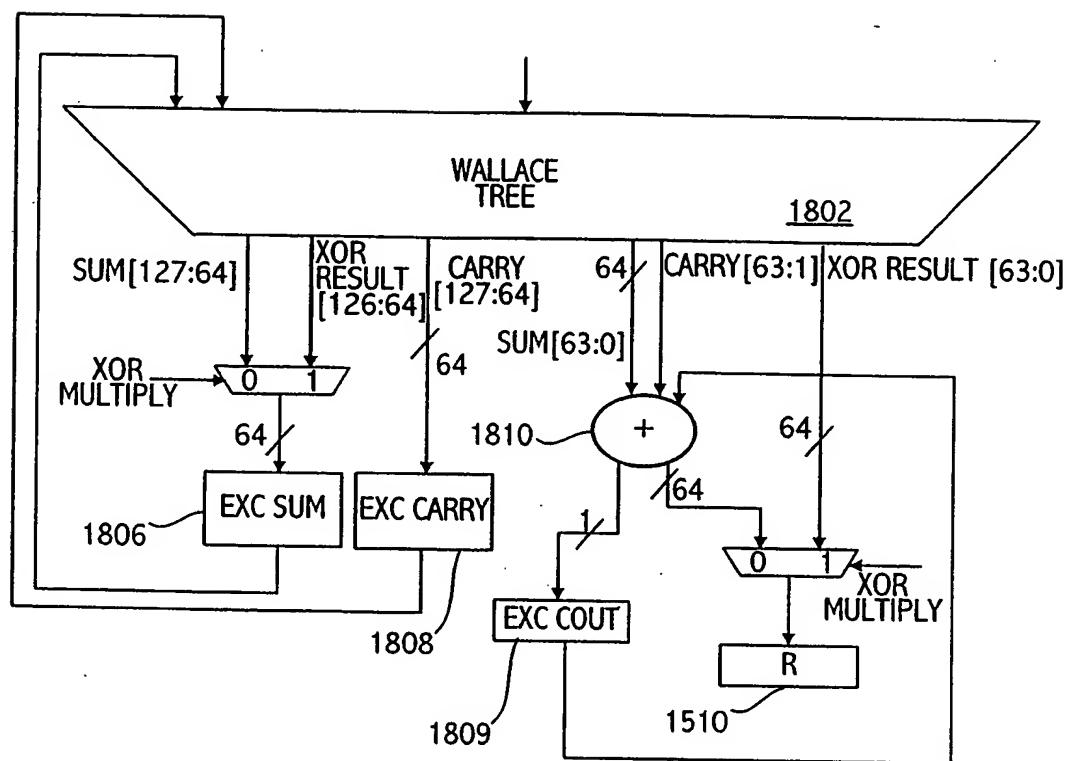


FIG. 19

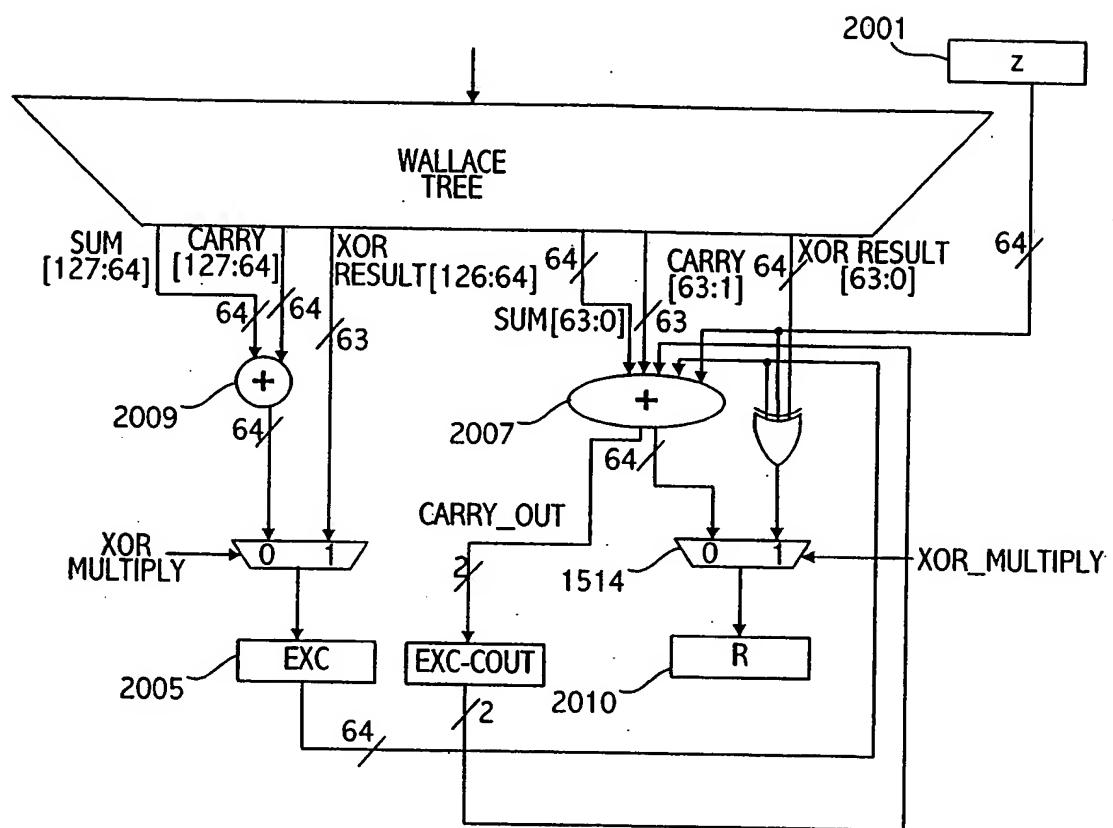


FIG. 20

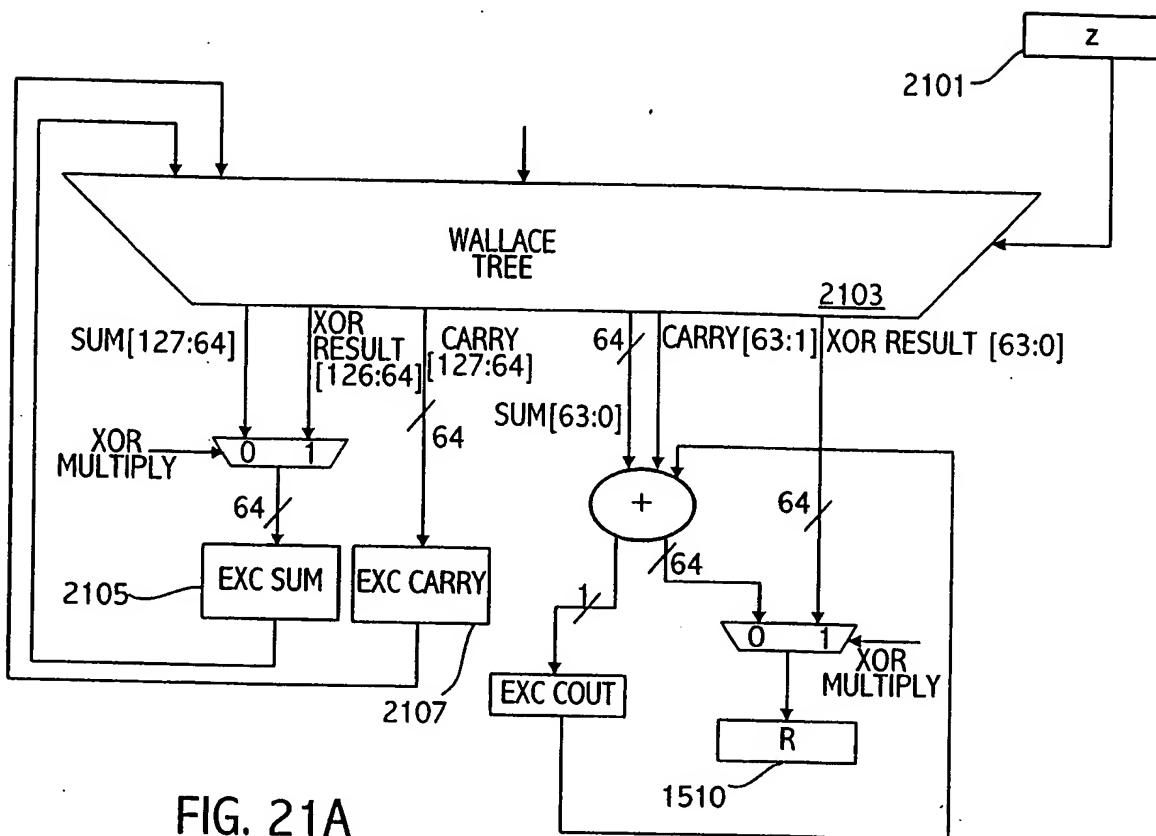


FIG. 21A

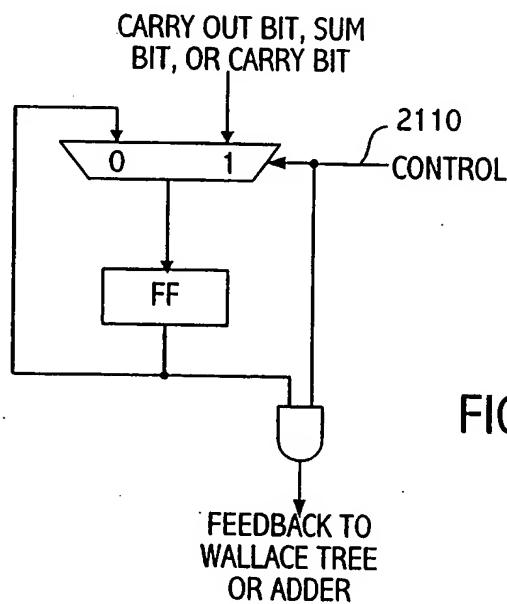


FIG. 21B

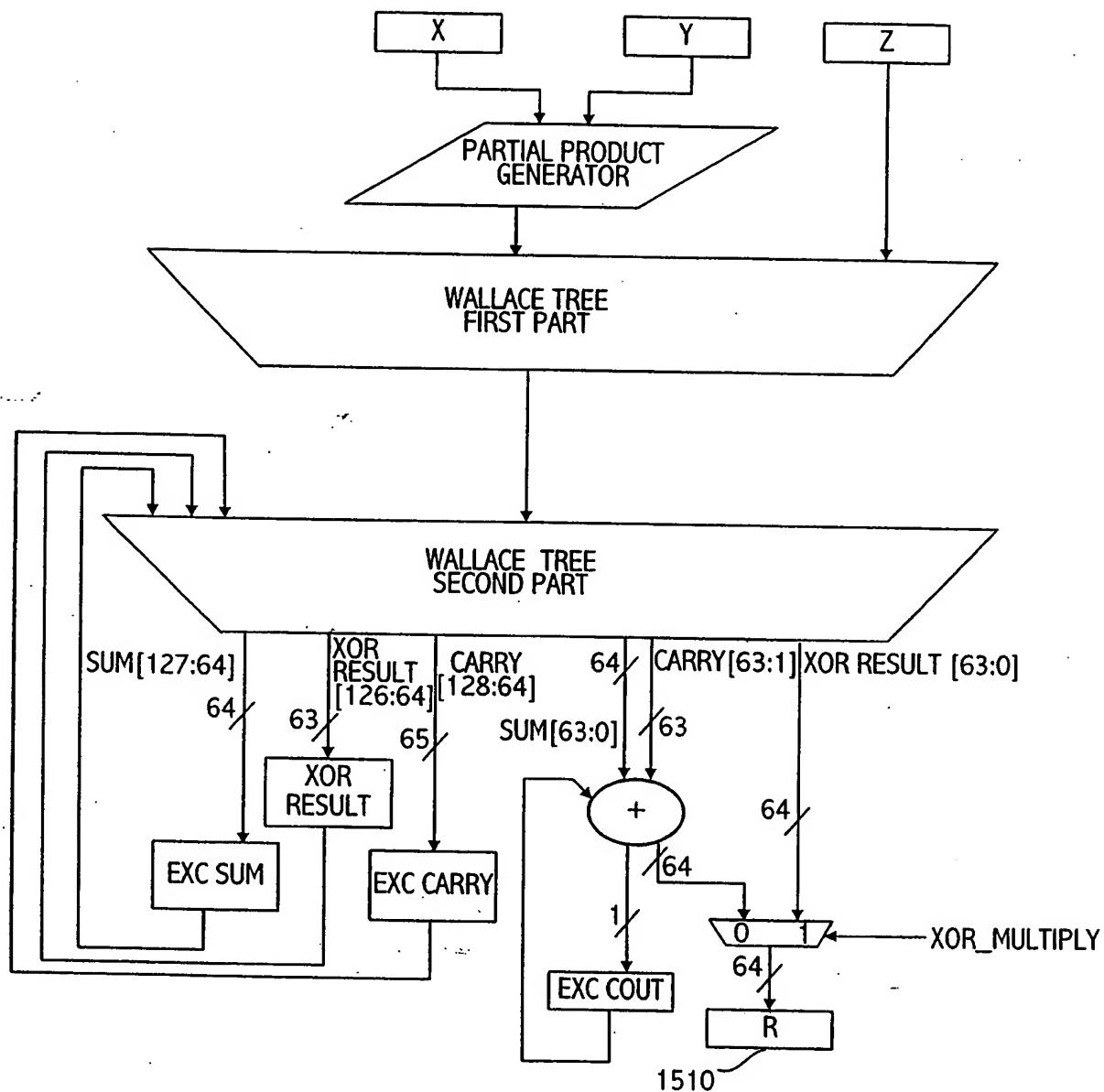
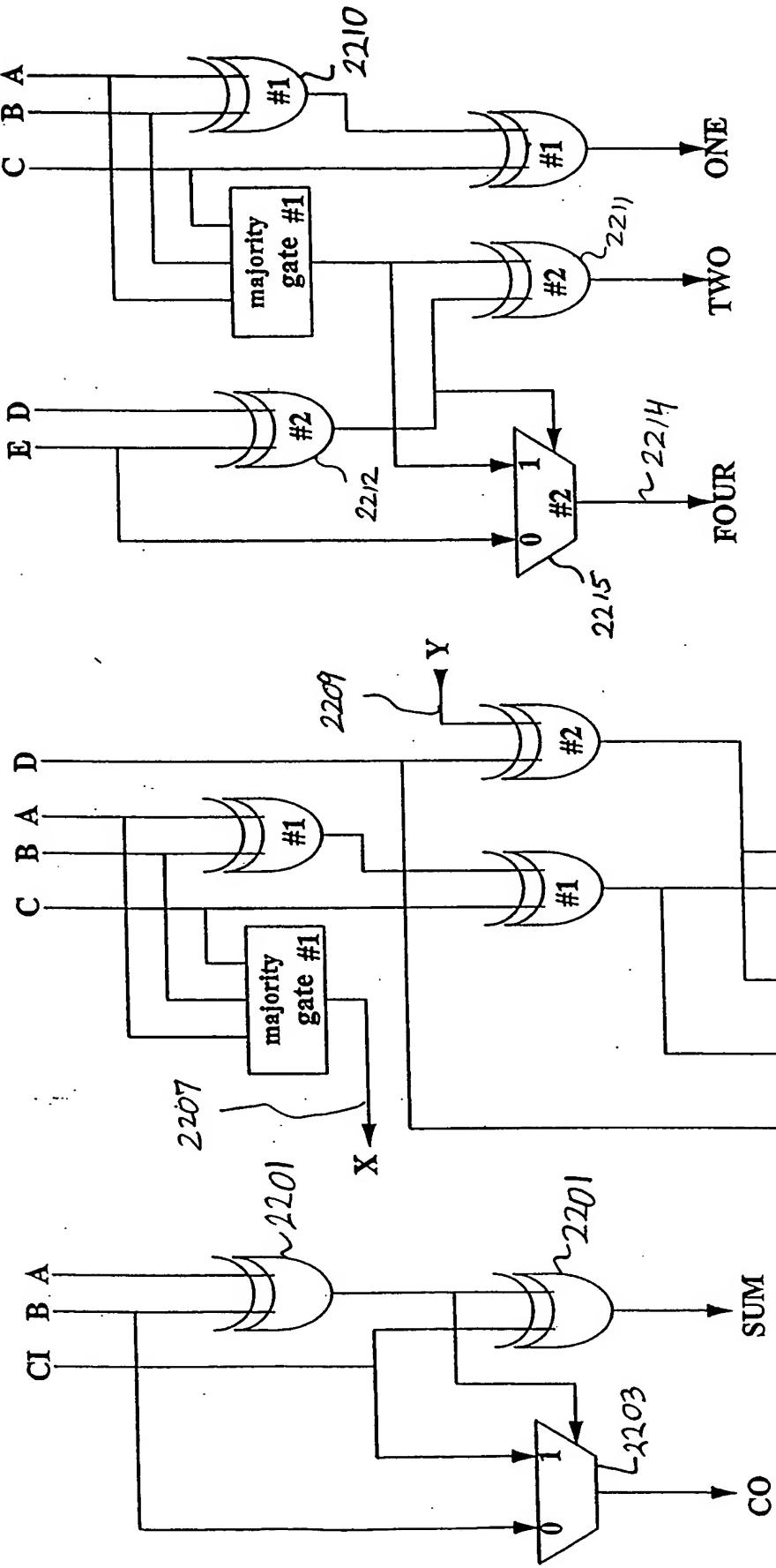


FIG. 21C

FULL ADDER COMPRESSOR 4 TO 2 5 TO 3



efficiency = 18.4%

efficiency = 18.4%

A	B	C	CI	CO	SUM	F_{14}
+ CO	+ Y	+ SUM	+ F14			

CO SUM ↓ CO SUM ↓ efficiency = 20.6%

SUM 1.6%

Fig. 22c

XOR MUX MAJORITY MAJORITy MUL

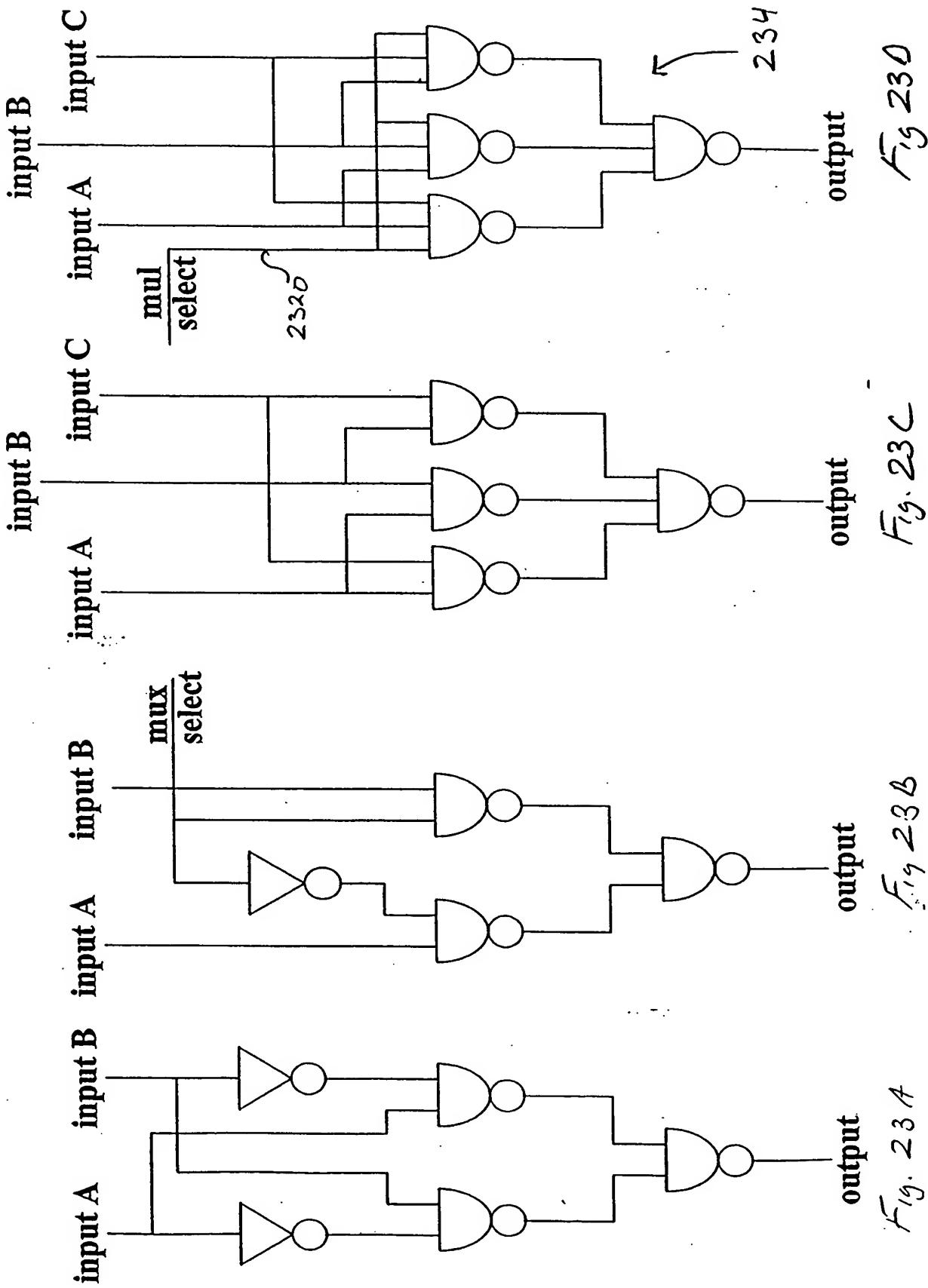


Fig. 23A

Fig. 23B

Fig. 23C

Fig. 23D

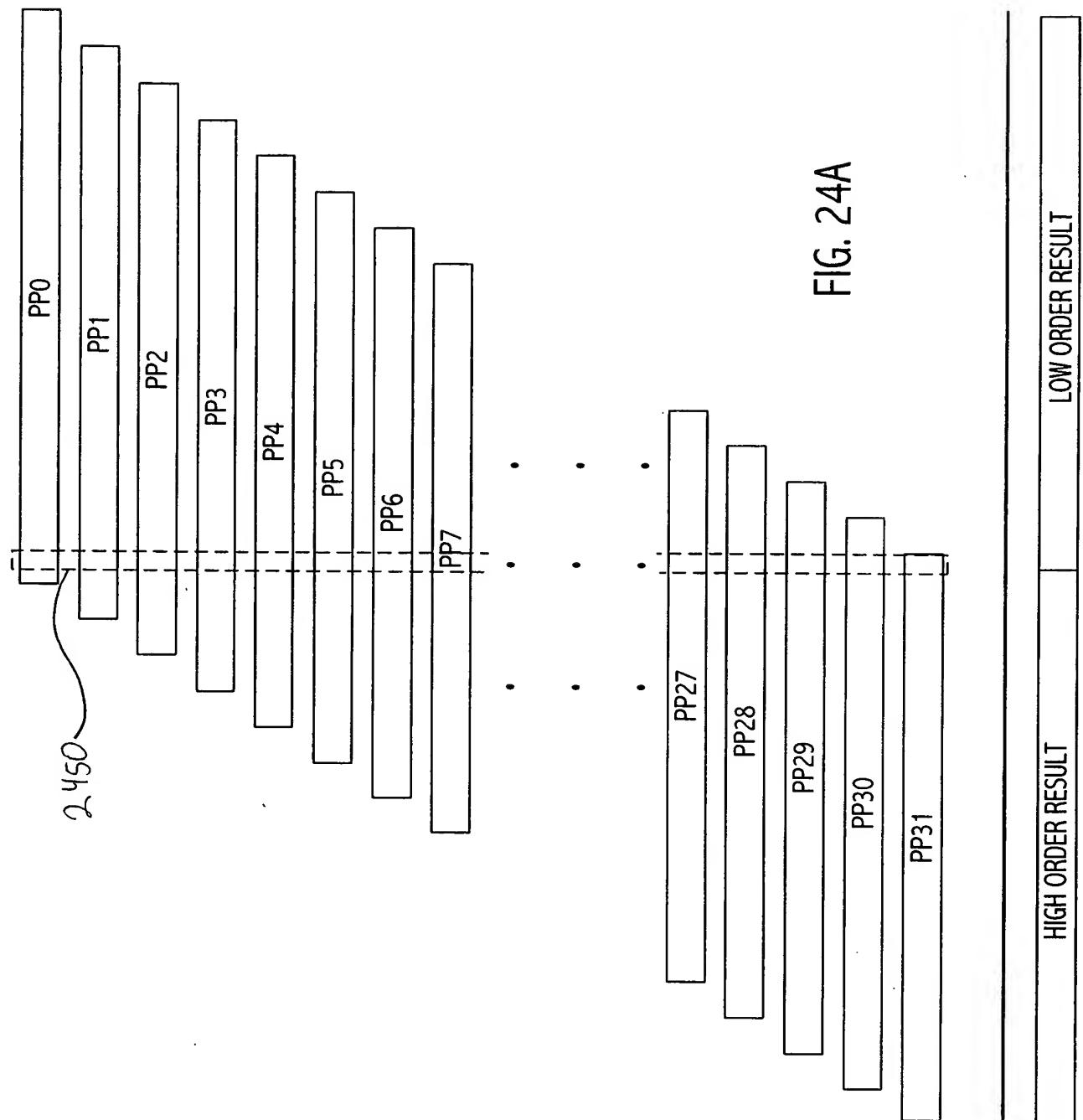
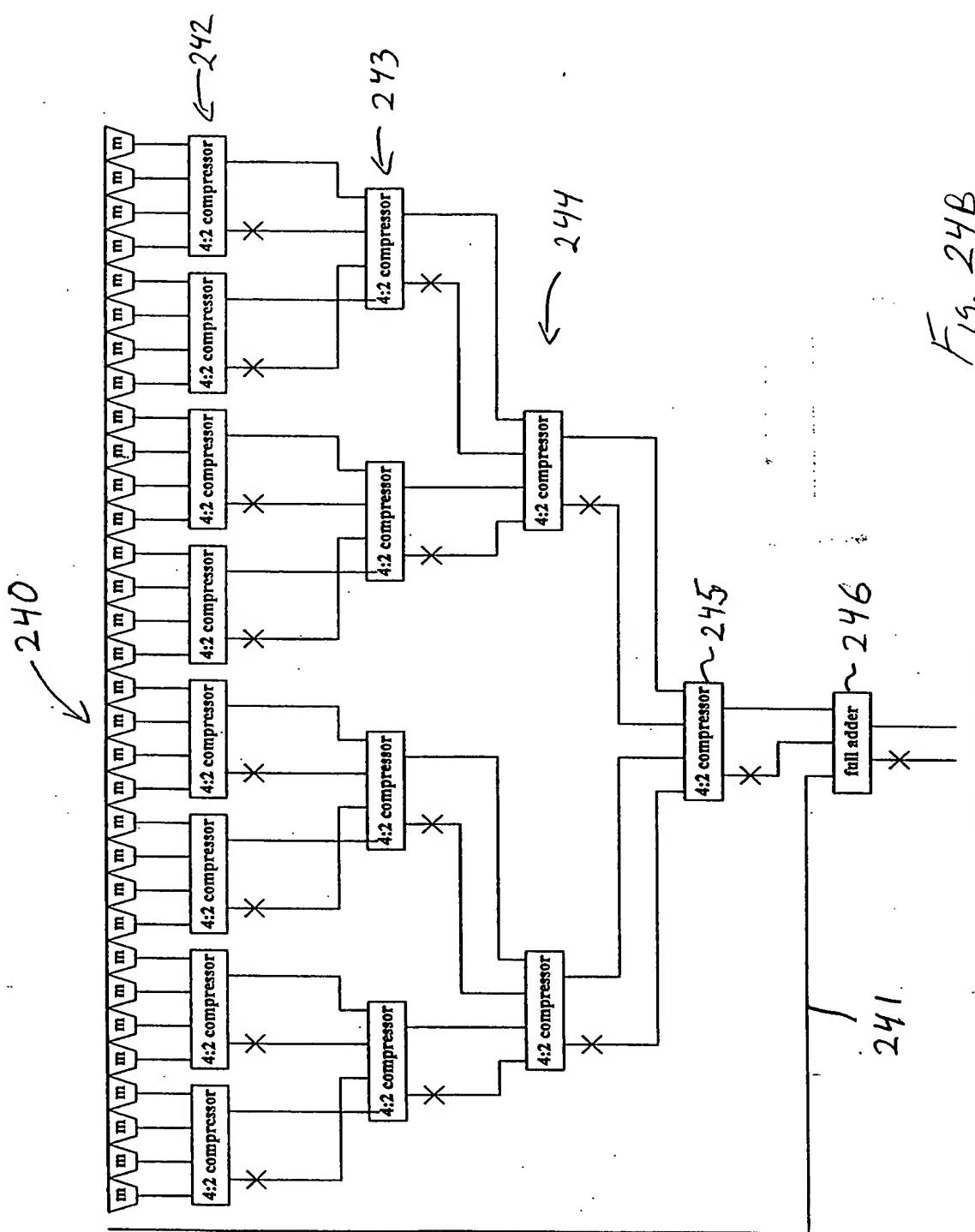
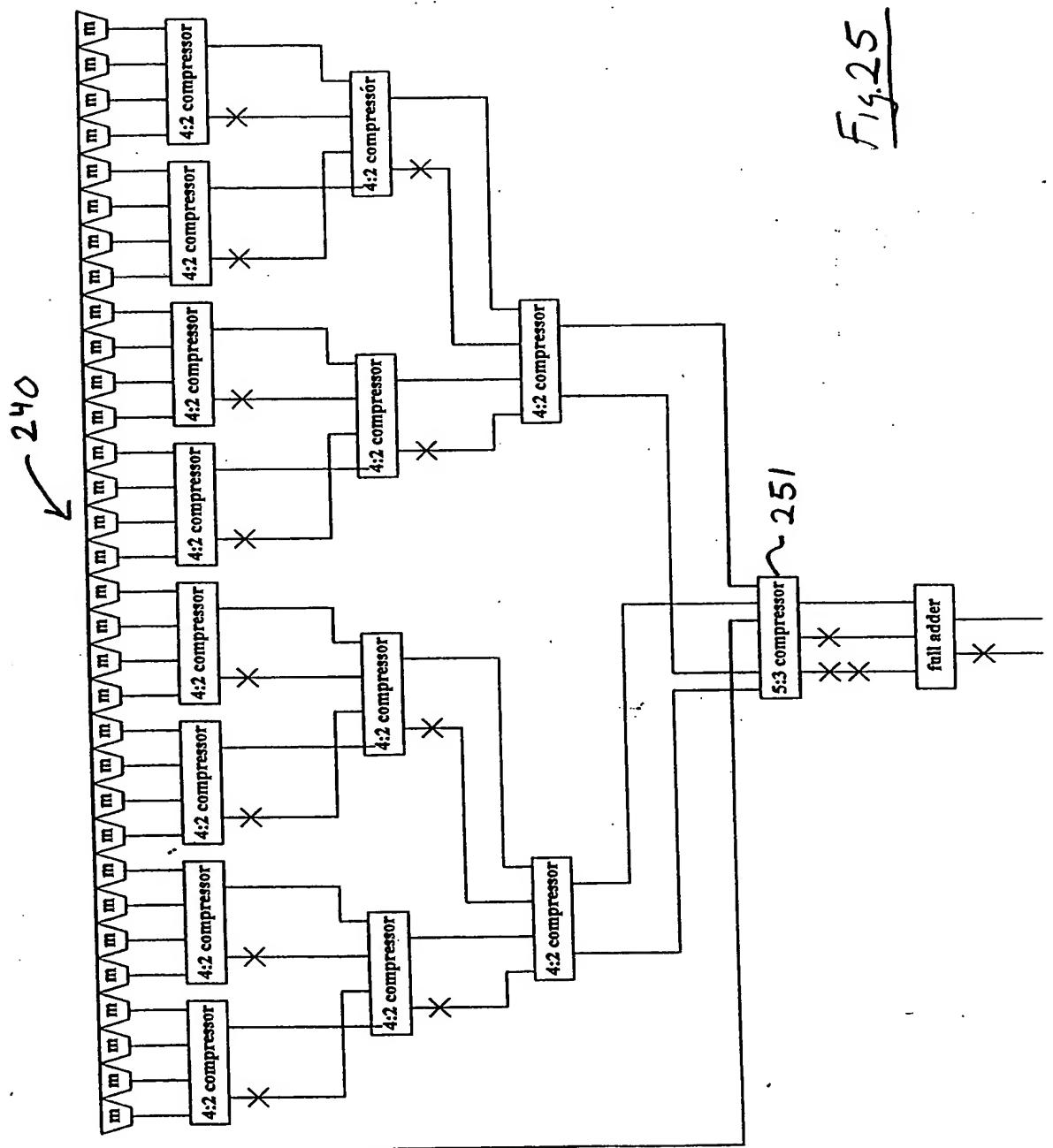
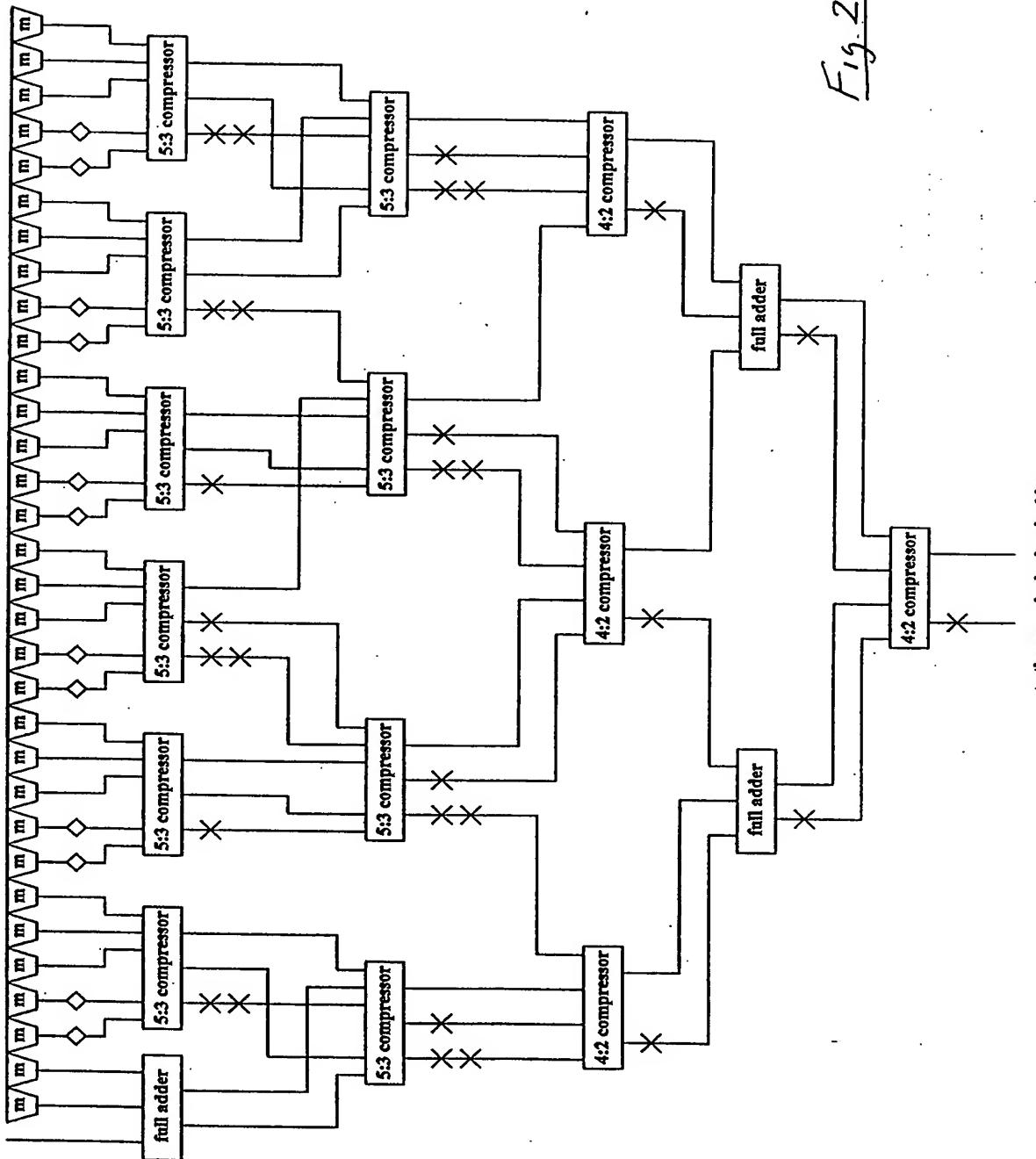


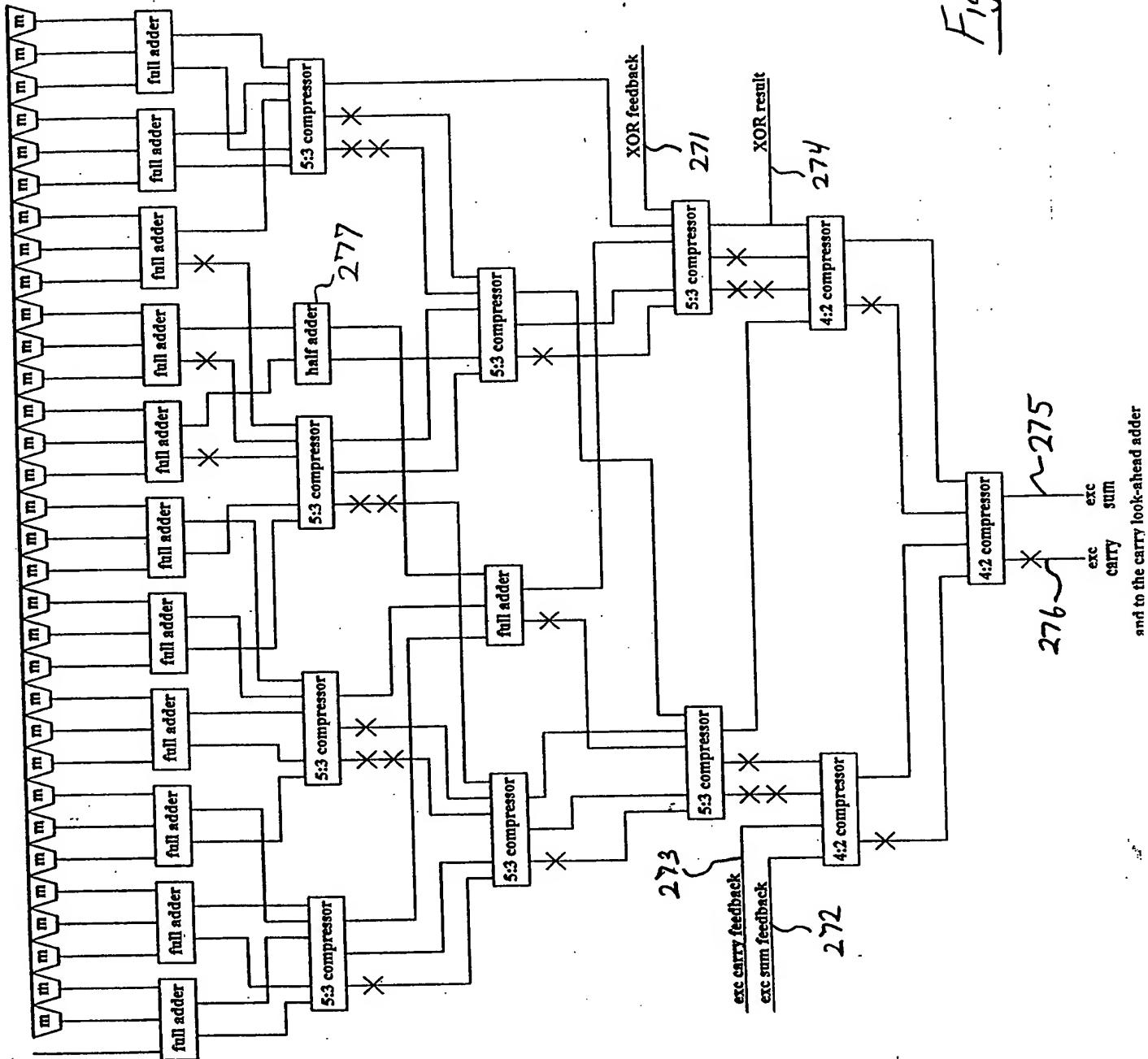
FIG. 24A





to the carry look-ahead adder





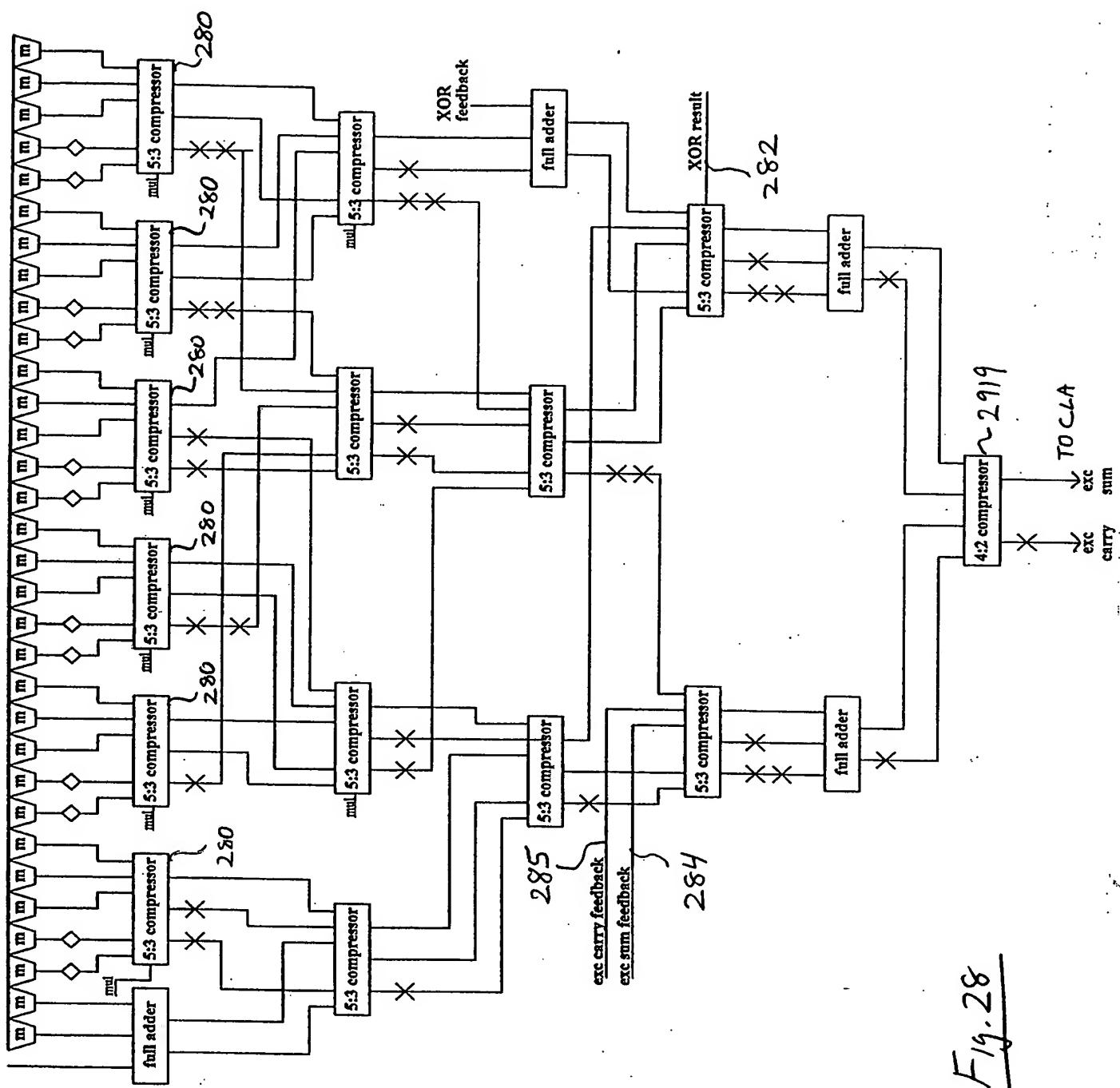
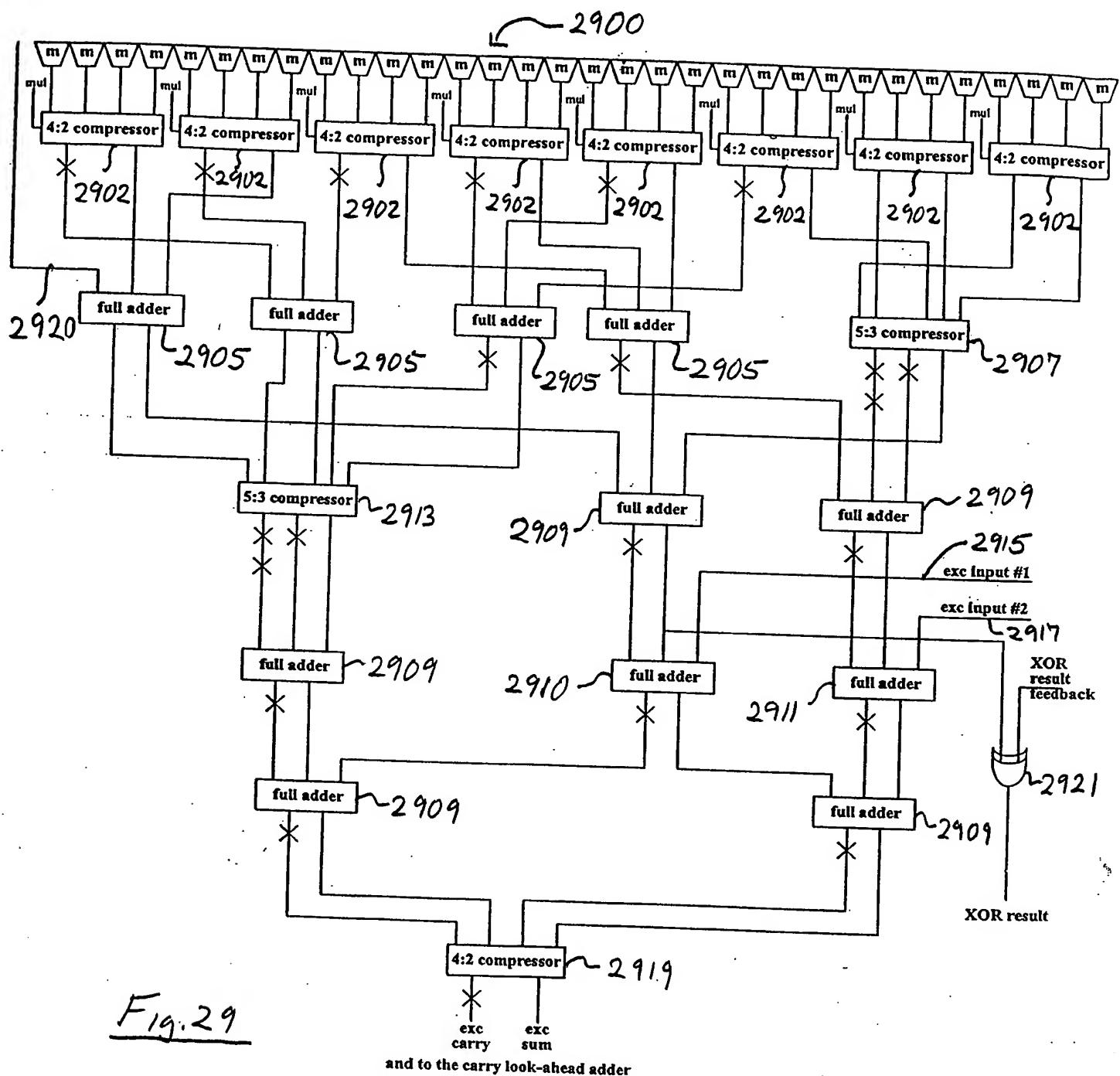


Fig. 28

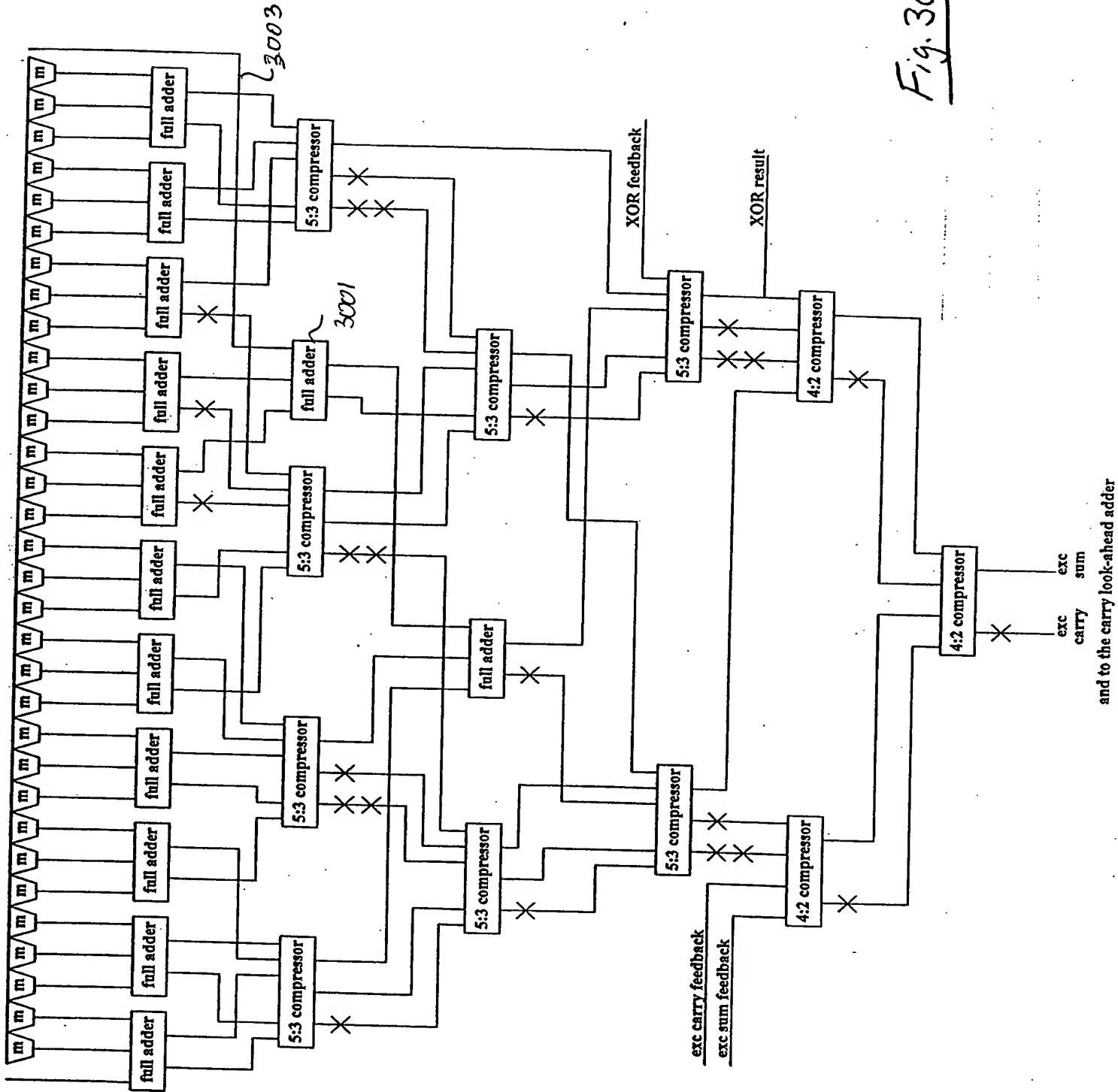


METHOD AND APPARATUS FOR IMPLEMENTING PROCESSOR
INSTRUCTIONS FOR ACCELERATING PUBLIC-KEY CRYPTOGRAPHY
Inventor(s): Sheueling Chang Shantz et al.

Inventor(s): Sheueling Chang Shantz et al

Atty. Dkt: No. 004-30132

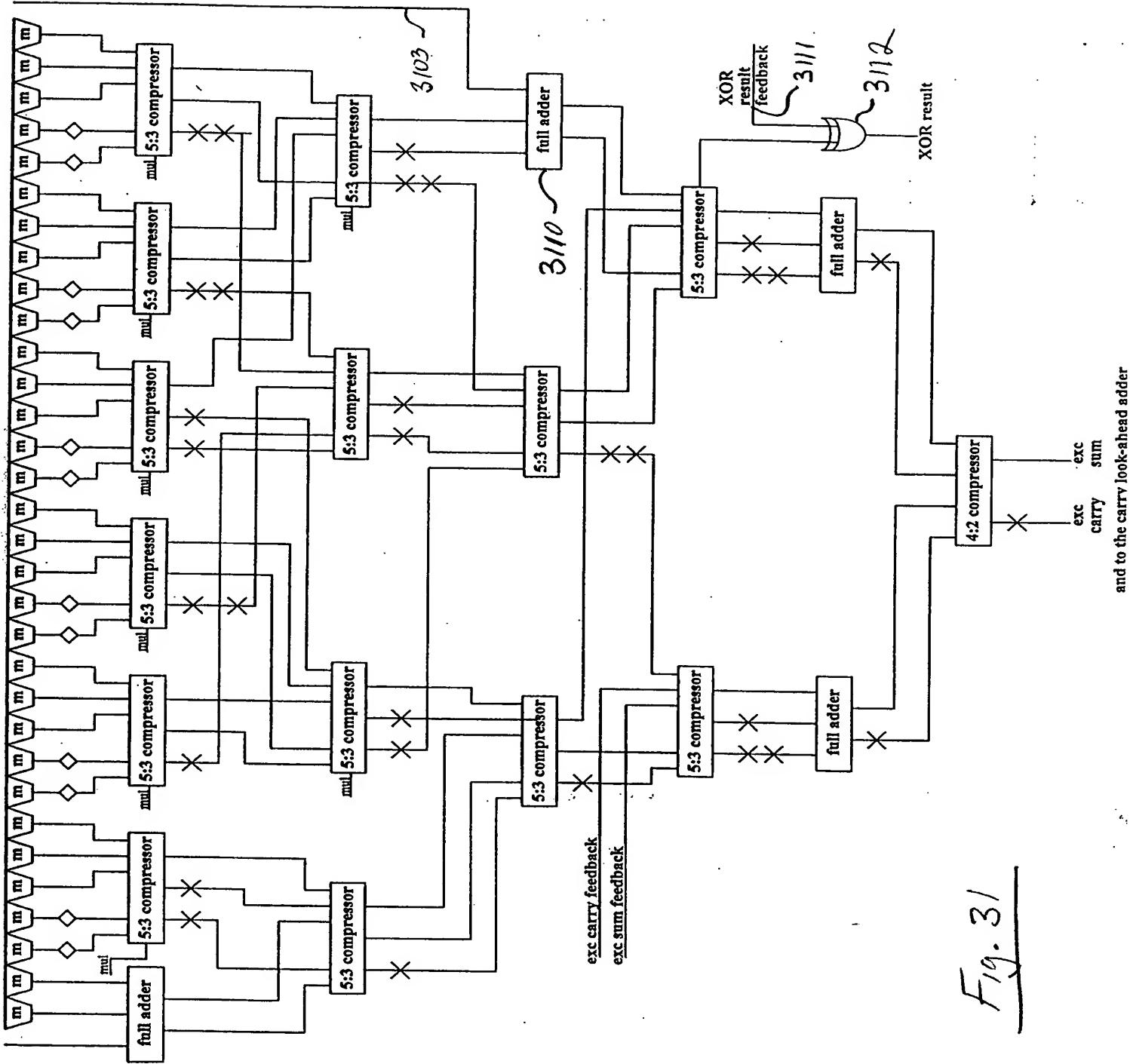
34/36

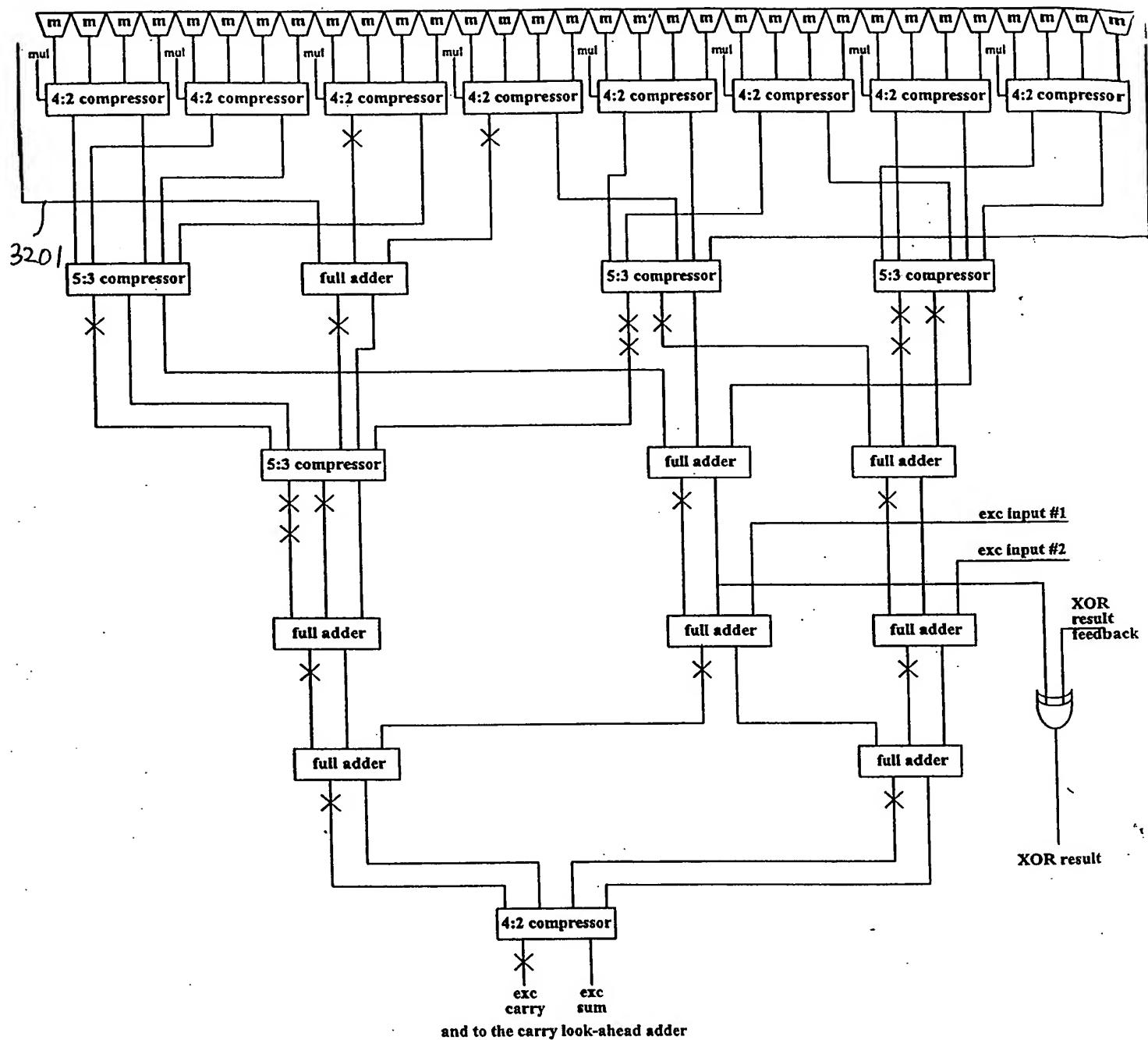


METHOD AND APPARATUS FOR IMPLEMENTING PROCESSOR
INSTRUCTIONS FOR ACCELERATING PUBLIC-KEY CRYPTOGRAPHY
Inventor(s): Sheueling Chang Shantz et al.

Atty. Dkt. No. 004-30132

35/36





and to the carry look-ahead adder

Fig. 32